ESET NOD32 ANTIVIRUS 5

User Guide

(intended for product version 5.0 and higher)

Microsoft® Windows® 7 / Vista / XP / 2000 / Home Server / NT4 (SP6)

Click here to download the most recent version of this document

ESET **NOD32 ANTIVIRUS**

Copyright ©2011 by ESET, spol. s r. o.
ESET NOD32 Antivirus was developed by ESET, spol. s r. o.
For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r. o. reserves the right to change any of the described application software without prior notice.

Worldwide Customer Support: www.eset.com/support

REV. 8/30/2011

Contents

1. ESET NOD32 Antivirus 5 5
1.1 What's new 5
1.2 System requirements 6
1.3 Prevention 6
2. Installation 8
2.1 Typical installation 9
2.2 Custom installation 12
2.3 Upgrading to a newer version 15
2.4 Entering username and password 15
2.5 Computer scan 16
3. Beginner's guide 17
3.1 Introducing user interface design 17
3.2 What to do if the program doesn't work properly 18
3.3 Update setup 19
3.4 Proxy server setup 20
3.5 Settings protection 21
4. Work with ESET NOD32 Antivirus 22
4.1 Computer 23
4.1.1 Antivirus and antispyware protection 24
4.1.1.1 Real-time file system protection 24
4.1.1.1.1 Media to scan 25
4.1.1.1.2 Scan on (Event-triggered scanning) 25
4.1.1.1.3 Advanced scan options 25
4.1.1.1.4 Cleaning levels 25
4.1.1.1.5 When to modify real-time protection configuration 26
4.1.1.1.6 Checking real-time protection 26
4.1.1.1.7 What to do if real-time protection does not work 26
4.1.1.2 Document protection 27
4.1.1.3 Computer scan 27
4.1.1.3.1 Type of scan 28
4.1.1.3.1.1 Smart scan 28
4.1.1.3.1.2 Custom scan 28
4.1.1.3.2 Scan targets 28
4.1.1.3.3 Scan profiles 29
4.1.1.3.4 Scan progress 29
4.1.1.4 Startup scan 30
4.1.1.5 Exclusions 31
4.1.1.6 ThreatSense engine parameters setup 32
4.1.1.6.1 Objects 32
4.1.1.6.2 Options 32
4.1.1.6.3 Cleaning 33
4.1.1.6.4 Extension 33
4.1.1.6.5 Limits 34
4.1.1.6.6 Other 34
4.1.1.7 An infiltration is detected 35
4.1.2 Removable media scanning and blocking 36
4.1.3 Host-based Intrusion Prevention System (HIPS) 36
4.2 Web and email 38
4.2.1 Web access protection 38
4.2.1.1 HTTP, HTTPs 39
4.2.1.1.1 Active mode for web browsers 39
4.2.1.2 URL address management 40
4.2.2 Email client protection 42
4.2.2.1 POP3, POP3S filter 43
4.2.2.2 IMAP, IMAPS protocol control 44
4.2.2.3 Integration with email clients 45
4.2.2.3.1 Email client protection configuration 45
4.2.2.4 Removing infiltrations 46
4.2.3 Protocol filtering 46
4.2.3.1 Excluded applications 46
4.2.3.2 Excluded addresses 47
4.2.3.3 SSL protocol checking 47
4.2.3.3.1 Certificates 48
4.2.3.3.1.1 Trusted certificates 49
4.2.3.3.1.2 Excluded certificates 49
4.3 Updating the program 49
4.3.1 Update setup 53
4.3.1.1 Update profiles 54
4.3.1.2 Advanced update setup 54
4.3.1.2.1 Update mode 54
4.3.1.2.2 Proxy server 55
4.3.1.2.3 Connecting to the LAN 56
4.3.2 How to create update tasks 57
4.4 Tools 58
4.4.1 Log files 59
4.4.1.1 Log maintenance 60
4.4.2 Scheduler 61
4.4.2.1 Creating new tasks 63
4.4.3 Protection statistics 64
4.4.4 Watch activity 65
4.4.5 ESET SysInspector 65
4.4.6 ESET Live Grid 66
4.4.6.1 Suspicious files 67
4.4.7 Running processes 68
4.4.8 Quarantine 69
4.4.8.1 Quarantining files 70
4.4.8.2 Restoring from Quarantine 70
4.4.8.3 Submitting file from Quarantine 70
4.4.9 Submission of files for analysis 71
4.4.10 System updates 71
4.4.11 Diagnostics 71
4.5 User interface 72
4.5.1 Graphics 72
4.5.2 Alerts and notifications 73
4.5.2.1 Advanced setup 74
4.5.3 Hidden notification windows 74
4.5.4 Access setup 75
4.5.5 Context menu 75
4.5.6 Gamer mode 76
5. Advanced user 77
5.1 Proxy server setup 77
5.2 Import and export settings 78
5.3 Keyboard shortcuts 79
5.4 Command Line 79
5.5 ESET SysInspector 80
5.5.1 Introduction to ESET SysInspector 80
5.5.1.1 Starting ESET SysInspector 81
5.5.2 User Interface and application usage 81
5.5.2.1 Program Controls 81
5.5.2.2 Navigating in ESET SysInspector 82
5.5.2.3 Compare 83
5.5.3 Command line parameters 84
5.5.4 Service Script 85
5.5.4.1 Generating Service script 85
5.5.4.2 Structure of the Service script 85
5.5.4.3 Executing Service scripts 88
5.5.5 Shortcuts 88
5.5.6 System requirements 89
5.5.7 FAQ 89
5.5.8 ESET SysInspector as part of ESET NOD32 Antivirus 90
5.6 ESET SysRescue 91
5.6.1 Minimun requirements 91
5.6.2 How to create rescue CD 91

5.6.3 Target selection ... 91
5.6.4 Settings ... 92
5.6.4.1 Folders ... 92
5.6.4.2 ESET Antivirus ... 92
5.6.4.3 Advanced settings ... 92
5.6.4.4 Internet protocol ... 93
5.6.4.5 Bootable USB device ... 93
5.6.4.6 Burn ... 93
5.6.5 Working with ESET SysRescue ... 93
5.6.5.1 Using ESET SysRescue ... 94

6. Glossary ... 95

6.1 Types of infiltration ... 95
6.1.1 Viruses ... 95
6.1.2 Worms ... 95
6.1.3 Trojan horses ... 95
6.1.4 Rootkits ... 96
6.1.5 Adware ... 96
6.1.6 Spyware ... 96
6.1.7 Potentially unsafe applications ... 96
6.1.8 Potentially unwanted applications ... 97

6.2 Email ... 97
6.2.1 Advertisements ... 97
6.2.2 Hoaxes ... 97
6.2.3 Phishing ... 98
6.2.4 Recognizing spam scams ... 98

1. ESET NOD32 Antivirus 5

ESET NOD32 Antivirus 5 represents a new approach to truly integrated computer security. The most recent version of the ThreatSense® scanning engine utilize speed and precision to keep your computer safe. The result is an intelligent system that is constantly on alert for attacks and malicious software endangering your computer.

ESET NOD32 Antivirus 5 is a complete security solution produced from our long-term effort to combine maximum protection and a minimal system footprint. The advanced technologies, based on artificial intelligence, are capable of proactively eliminating infiltration by viruses, spyware, trojan horses, worms, adware, rootkits, and other Internet-borne attacks without hindering system performance or disrupting your computer.

1.1 What's new

HIPS

Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys, actively blocking and preventing any such attempts.

Join ESET Live Grid network

Built on ThreatSense.net advanced early warning system, ESET Live Grid is designed to provide additional levels of security to your computer. It constantly monitors your system's running programs and processes against the latest intelligence collected from millions of ESET users worldwide. Additionally, your system scans are processed faster and more precisely as the ESET Live Grid database grows over time. This allows us to offer greater proactive protection and speed of scanning to all our users. We recommend that you activate this feature and we thank you for your support.

Removable media control

ESET NOD32 Antivirus provides removable media (CD/DVD/USB/...) control. This module allows you to scan, block or adjust extended filters/permissions and control how the user can access and work with a given device. This may be useful if the computer administrator wishes to prevent removable media insertion with unsolicited content by users.

Gamer mode

Gamer mode is a feature for gamers that demand uninterrupted usage of their software, do not wish to be disturbed by pop-up windows and want to minimize CPU usage. Gamer mode can also be used as a presentation mode, when a presentation cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled and the activity of the scheduler will be completely stopped. System protection still runs in the background but does not demand any user interaction.

Check for product updates

ESET NOD32 Antivirus can be configured, in addition to virus signature database updates and program modules updates, to check regularly for the latest product version. During the installation process, using an older installation package, you can decide if you want to automatically download and install the latest version of ESET NOD32 Antivirus.

New design

The main window of ESET NOD32 Antivirus has been completely redesigned and Advanced Setup is more intuitive for easier navigation.

1.2 System requirements

For seamless operation of ESET NOD32 Antivirus, the system should meet the following hardware and software requirements:

Microsoft® Windows® 2000, XP, NT4 (SP6)

400 MHz 32-bit (x86) / 64-bit (x64)
128MB RAM of system memory
320 MB available space
Super VGA (800 x 600)

Microsoft® Windows® 7, Vista, Home Server

1 GHz 32-bit (x86) / 64-bit (x64)
512MB RAM of system memory
320 MB available space
Super VGA (800 x 600)

1.3 Prevention

When you work with your computer, and especially when you browse the Internet, please keep in my mind that no antivirus system in the world can completely eliminate the risk caused by infiltrations and attacks. To provide maximum protection and convenience, it is essential to use the antivirus system correctly and adhere to several useful rules.

Update regularly

According to the statistics from ESET Live Grid, thousands of new, unique infiltrations are created each day in order to bypass existing security measures and bring profit to their authors – all at the expense of other users. The specialists at ESET's Virus Lab analyze those threats on a daily basis and prepare and release updates in order to continually improve the level of protection for users of the antivirus program. An incorrectly configured update decreases the effectiveness of the program. For more information on how to configure updates, click here.

Download security patches

The authors of malicious software prefer exploiting various system vulnerabilities in order to increase the effectiveness of spreading malicious code. That's why software companies watch closely for new vulnerabilities in their applications to appear and release security updates eliminating potential threats on a regular basis. It's important to download these security updates as they are released. Examples of such applications include the windows operating system or widely-used internet browser Internet Explorer.

Backup important data

Malware writers usually do not care about users' needs, and the activity of malicious programs often leads to total malfunction of the operating system and the deliberate damage of important data. It is important to regularly backup your important and sensitive data to an external source such as a DVD or external hard drive. Precautions such as these make it far easier and faster to recover your data in the event of system failure.

Regularly scan your computer for viruses

A regular automatic scan of your computer with the proper settings can remove infiltrations that may have been missed due to your computer containing old virus signature updates.

Follow basic security rules

This is the most useful and most effective rule of all – always be cautious. Today, many infiltrations require user intervention in order to be executed and distributed. If you are cautious when opening new files, you will save considerable time and effort that would otherwise be spent cleaning infiltrations from your computer. Some useful rules are:

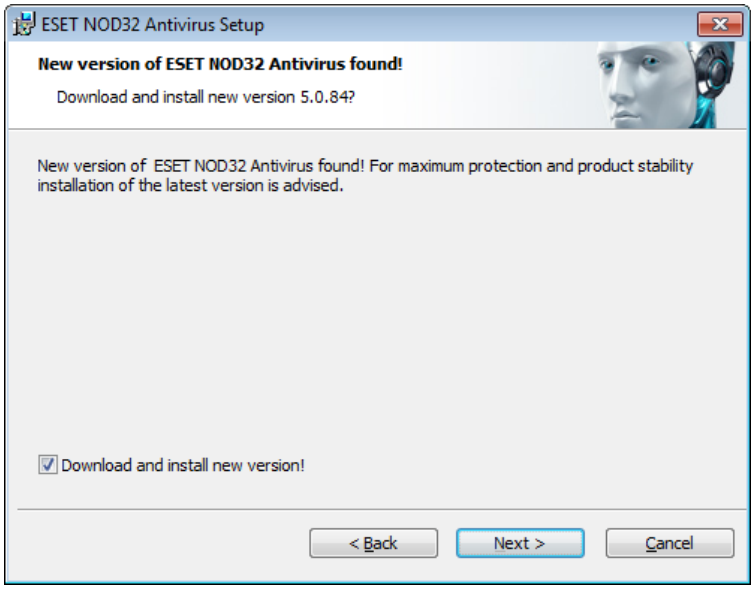
- Do not visit suspicious websites with multiple pop-ups and flashing advertisements.
- Be careful when installing freeware programs, codec packs, etc. Only use safe programs and only visit safe Internet websites.
- Be cautious when opening email attachments, particularly those from mass-mailed messages and messages from unknown senders.
- Don't use an Administrator account for everyday work with your computer.

2. Installation

Once you launch the installer, the installation wizard will guide you through the basic setup process.

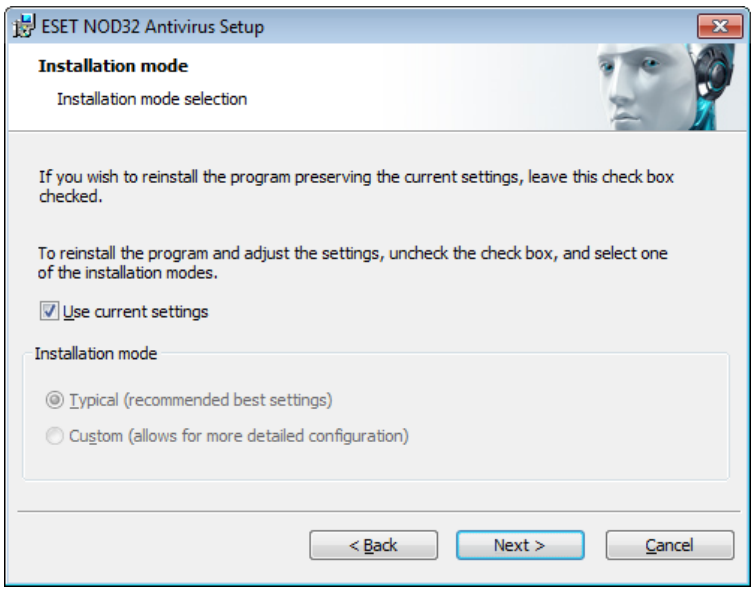
Important: Make sure that no other antivirus programs are installed on your computer. If two or more antivirus solutions are installed on a single computer, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system. See also our knowledgebase article (available in English and several other languages).

First, the program checks if a newer version of ESET NOD32 Antivirus is available. If a newer version is found, you will see the following window:

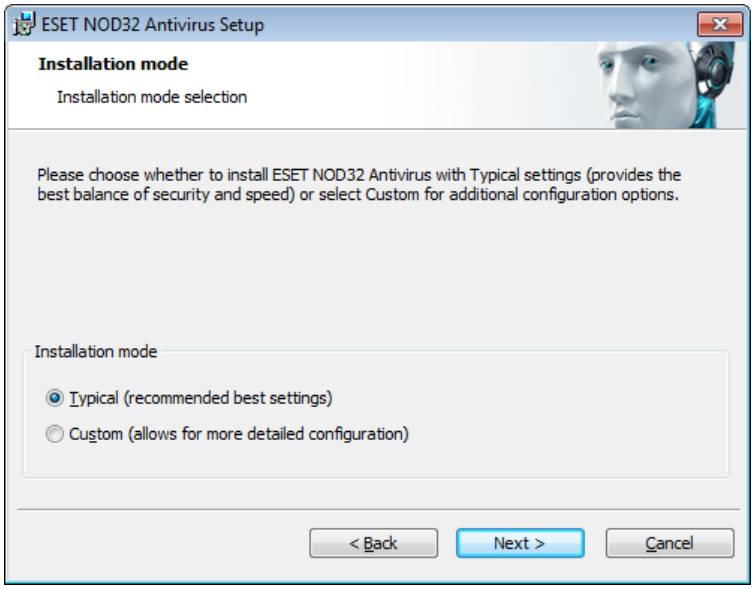

ESET NOD32 Antivirus Setup
New version of ESET NOD32 Antivirus found!
Download and install new version 5.0.84?
New version of ESET NOD32 Antivirus found! For maximum protection and product stability installation of the latest version is advised.
Download and install new version!
< Back
Next >
Cancel

If you select the **Download and install new version** option, the new version will be downloaded and the installation will continue. In the next step the End-User License Agreement will be displayed. Please read and click **Accept** to acknowledge your acceptance of the End-User License Agreement. After you accept the installation will continue in two possible scenarios:

1. Installation of the ESET NOD32 Antivirus over a previous version of this software. The following window lets you choose to either use your current program settings for your new installation, or, if you uncheck the **Use current settings** option, you will be able to choose between the Typical installation and the Custom installation modes.


ESET NOD32 Antivirus Setup
Installation mode
Installation mode selection
If you wish to reinstall the program preserving the current settings, leave this check box checked.
To reinstall the program and adjust the settings, uncheck the check box, and select one of the installation modes.
Use current settings
Installation mode
Typical (recommended best settings)
Custom (allows for more detailed configuration)
< Back
Next >
Cancel

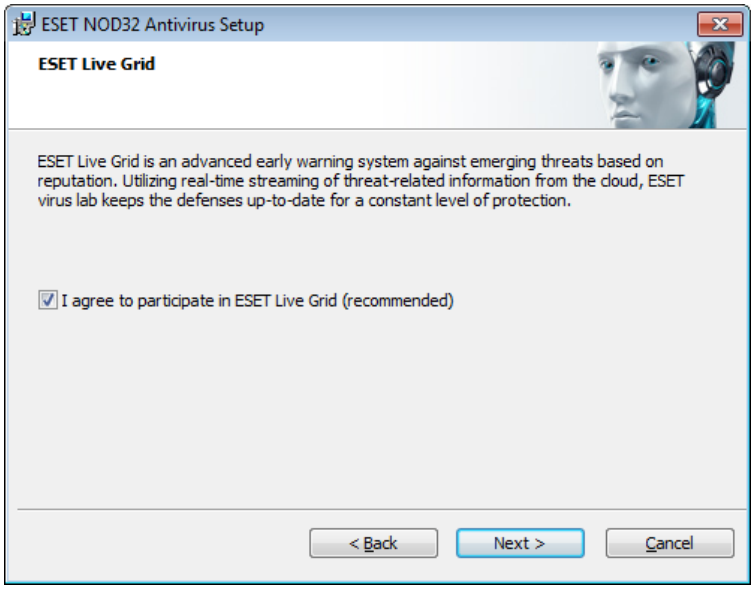
2. If you are installing ESET NOD32 Antivirus on a computer without a previous version of the program, you will see the window below, after you accept the **End-User License Agreement**. Here, you can choose between a Typical installation and a Custom installation and continue accordingly.


ESET NOD32 Antivirus Setup
Installation mode
Installation mode selection
Please choose whether to install ESET NOD32 Antivirus with Typical settings (provides the best balance of security and speed) or select Custom for additional configuration options.
Installation mode
Typical (recommended best settings)
Custom (allows for more detailed configuration)
< Back
Next >
Cancel

2.1 Typical installation

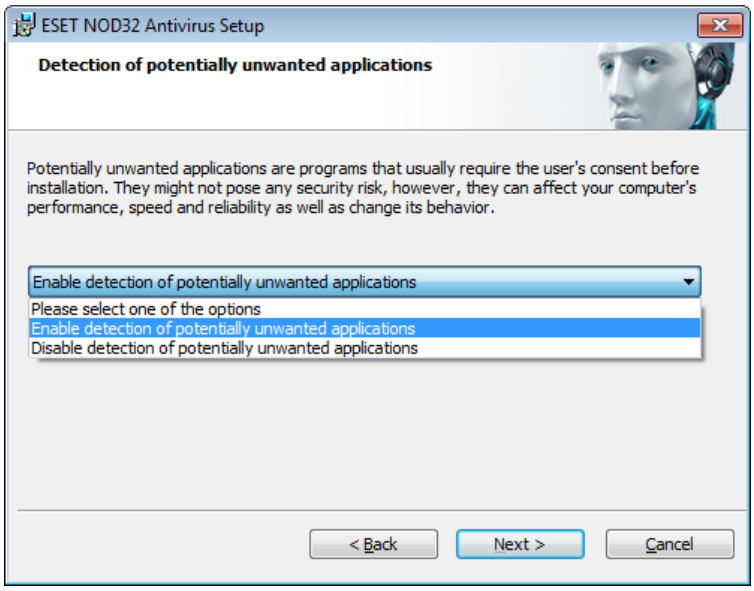
Typical installation mode provides configuration options appropriate for most users. These settings provide excellent security, easy setup and high system performance. Typical installation mode is the default option and is recommended if you do not have the particular requirements for specific settings.

After selecting the installation mode and clicking **Next**, you will be prompted to configure the ESET Live Grid. The ESET Live Grid helps to ensure that ESET is immediately and continuously informed about new infiltrations in order to quickly protect our customers. The system allows you to submit new threats to ESET's Virus Lab, where they are analyzed, processed and added to the virus signature database.


ESET NOD32 Antivirus Setup
ESET Live Grid
ESET Live Grid is an advanced early warning system against emerging threats based on reputation. Utilizing real-time streaming of threat-related information from the cloud, ESET virus lab keeps the defenses up-to-date for a constant level of protection.
I agree to participate in ESET Live Grid (recommended)
< Back
Next >
Cancel

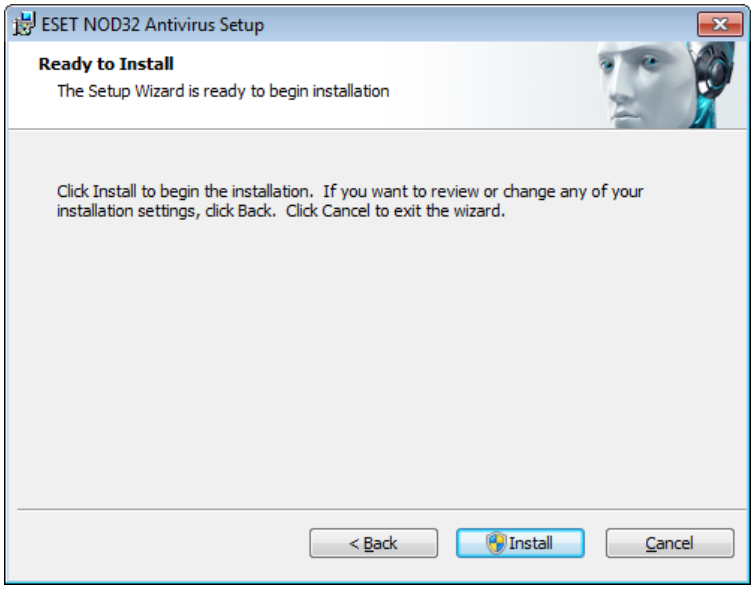
By default, the **I agree to participate in ESET Live Grid** option is selected, which will activate this feature.

The next step in the installation process is to configure detection of potentially unwanted applications. Potentially unwanted applications are not necessarily malicious, but can often negatively affect the behavior of your operating system. See the Potentially unwanted applications chapter for more details.


ESET NOD32 Antivirus Setup
Detection of potentially unwanted applications
Potentially unwanted applications are programs that usually require the user's consent before installation. They might not pose any security risk, however, they can affect your computer's performance, speed and reliability as well as change its behavior.
Enable detection of potentially unwanted applications
Please select one of the options
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications
< Back
Next >
Cancel

Select the **Enable detection of potentially unwanted applications** option to allow ESET NOD32 Antivirus to detect this type of applications.

The final step in Typical installation mode is to confirm installation by clicking the **Install** button.


ESET NOD32 Antivirus Setup
Ready to Install
The Setup Wizard is ready to begin installation
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< Back
Install
Cancel

After the installation is completed, you will be prompted to activate your product.

If you purchased a retail boxed version of the product, it already contains an Activation Key along with step-by-step activation instructions. The Activation Key is usually located inside or on the back side of the product package. For a successful activation, the Activation Key must be entered as supplied.

If you received a Username and Password, select the **Activate using a Username and Password** option and enter the license data in the appropriate fields.

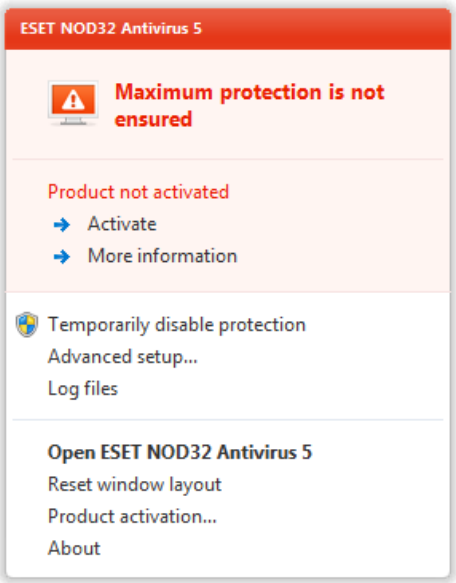
If you would like to evaluate ESET NOD32 Antivirus before making a purchase, select the **Activate Trial License** option. Fill in your email address and country to activate ESET NOD32 Antivirus for a limited time. Your test license will be emailed to you. Trial licenses can only be activated once per customer.

If you do not have a license and would like to buy one, click the **Purchase License** option. This will redirect you to the website of your local ESET distributor.

Product Activation
Product Activation Type
Important! Choose an option below to activate your ESET security product. Your product must be activated to ensure maximum protection.
Activate using an Activation Key (recommended)
Select this option if you purchased a CD or download version and have a 12, 13 or 20-digit activation key.
Activate using a Username and Password
Select this option if you received license email with your Username and Password.
Activate Trial License
Select this option if you would like to use and evaluate this product.
?
Purchase License
< Back
Next >
Activate Later

Select the **Activate Later** option if you would like to quickly evaluate our product and do not wish to activate it immediately.

You can also activate your copy of ESET NOD32 Antivirus directly from the program. Click the ESET NOD32 Antivirus icon located in the top right corner or right-click ESET NOD32 Antivirus system tray icon and then click **Product activation...** from the menu.



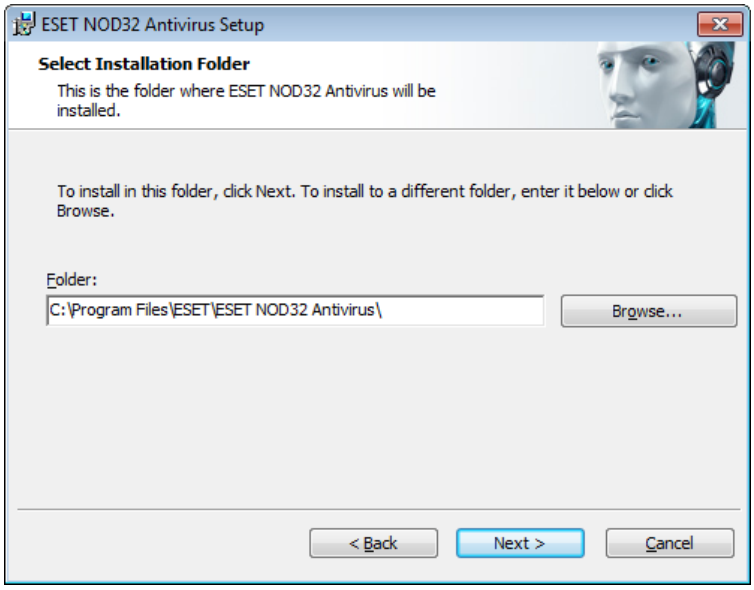
2.2 Custom installation

Custom installation mode is designed for users who have experience with fine-tuning programs and who wish to modify advanced settings during installation.

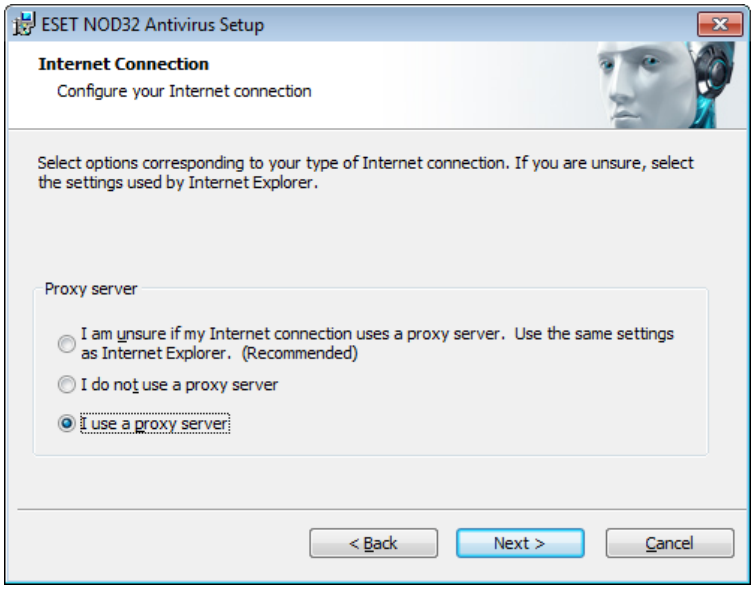
After selecting this installation mode and clicking **Next**, you will be prompted to select a destination location for the installation. By default, the program installs in:

C:\Program Files\ESET\ESET NOD32 Antivirus

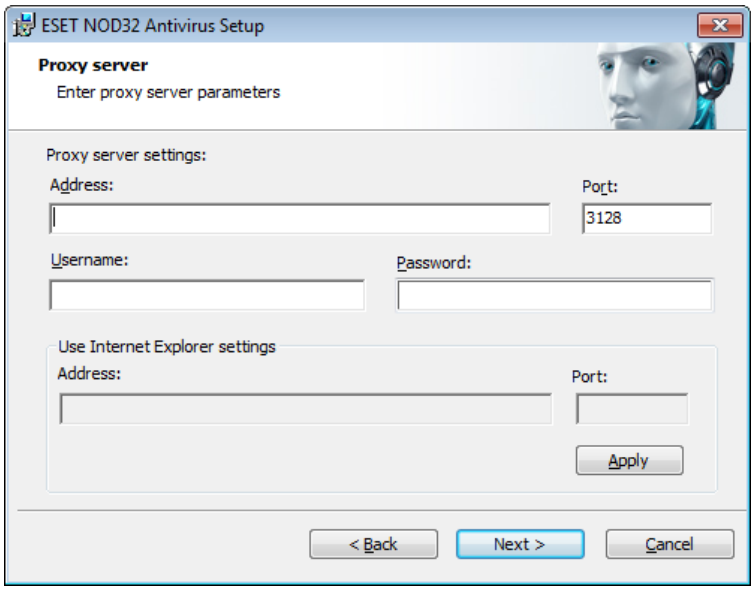
Click **Browse...** to change this location (not recommended).


ESET NOD32 Antivirus Setup
Select Installation Folder
This is the folder where ESET NOD32 Antivirus will be installed.
To install in this folder, click Next. To install to a different folder, enter it below or click Browse.
Folder:
C:\Program Files\ESET\ESET NOD32 Antivirus\
Browse...
< Back
Next >
Cancel

After entering your username and password, click **Next** and proceed to configuring your Internet connection.

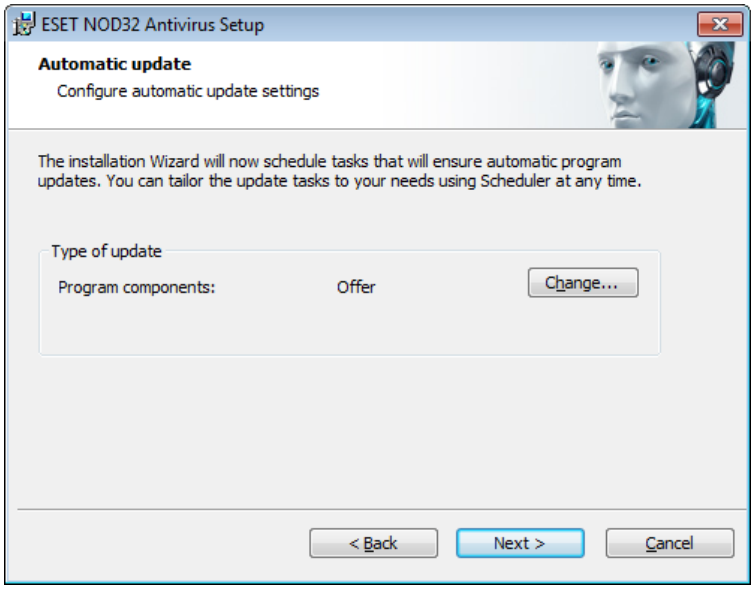

ESET NOD32 Antivirus Setup
Internet Connection
Configure your Internet connection
Select options corresponding to your type of Internet connection. If you are unsure, select the settings used by Internet Explorer.
Proxy server
I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer. (Recommended)
I do not use a proxy server
I use a proxy server
< Back
Next >
Cancel

If you use a proxy server, it must be correctly configured for virus signature updates to work. If you are not sure whether you use a proxy server to connect to the Internet, select the **I am unsure if my Internet connection uses a proxy server option. Use the same settings as Internet Explorer (Recommended)** and click **Next**. If you do not use a proxy server, select the **I do not use a proxy server** option.

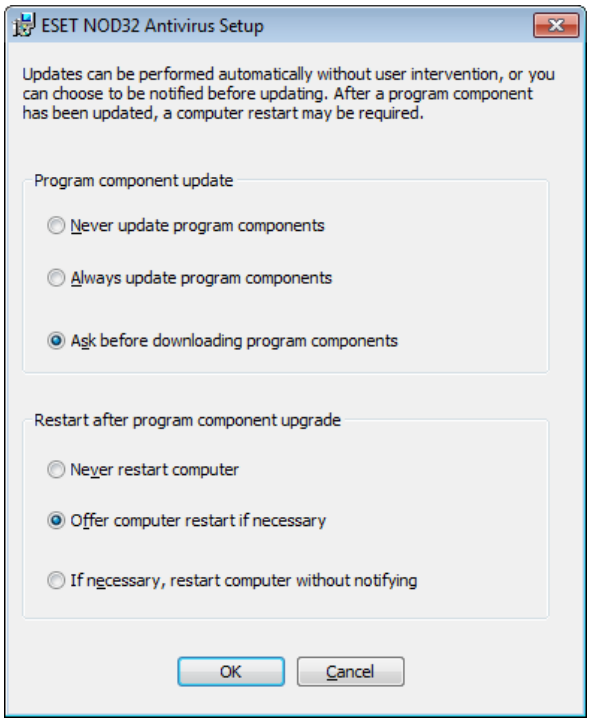


To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field. In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). In the event that the proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. To do this, click **Apply** and confirm the selection.

This installation step allows you to designate how automatic program updates will be handled on your system. Click **Change...** to access the advanced settings.

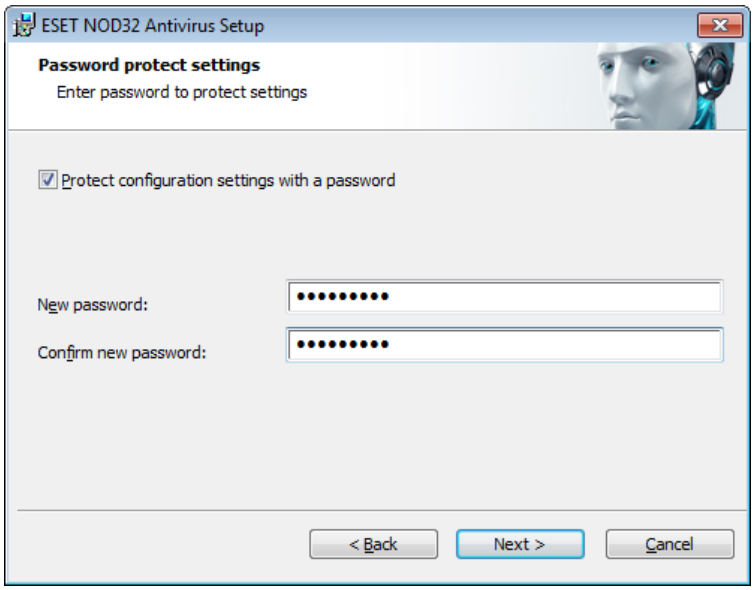

ESET NOD32 Antivirus Setup
Automatic update
Configure automatic update settings
The installation Wizard will now schedule tasks that will ensure automatic program updates. You can tailor the update tasks to your needs using Scheduler at any time.
Type of update
Program components:
Offer
Change...
< Back
Next >
Cancel

If you do not want program components to be updated, select the **Never update program components** option. Select the **Ask before downloading program components** option to display a confirmation window each time the system attempts to download program components. To download program component upgrades automatically, select the **Always update program components** option.


ESET NOD32 Antivirus Setup
Updates can be performed automatically without user intervention, or you can choose to be notified before updating. After a program component has been updated, a computer restart may be required.
Program component update
Never update program components
Always update program components
Ask before downloading program components
Restart after program component upgrade
Never restart computer
Offer computer restart if necessary
If necessary, restart computer without notifying
OK
Cancel

NOTE: After a program component update, a restart is usually required. We recommend selecting the **If necessary, restart computer without notifying** option.

The next installation window offers the option to set a password to protect your program settings. Select the **Protect configuration settings with a password** option and choose a password to enter in the **New password** and **Confirm new password** fields, which will be required to change or access the settings of ESET NOD32 Antivirus. When both password fields match, to click **Next** to continue.



The next two installation steps, **ESET community online service ESET Live Grid** and **Detection of potentially unwanted applications** are handled the same as in the Typical installation mode (see "Typical installation").

Click **Install** in the **Ready to install** window to complete installation. After the installation is completed, you will be prompted to activate your product. See typical installation for more information about product activation.

2.3 Upgrading to a newer version

Newer versions of ESET NOD32 Antivirus are issued to bring improvements or fix issues that cannot be resolved by automatically updating of the program modules. Upgrading to a newer version can be accomplished in several ways:

1. Automatically, by means of a program update
   Since the program upgrade is distributed to all users and may have impact on certain system configurations, it is issued after a long testing period to function with all possible system configurations. If you need to upgrade to a newer version instantly after it has been released, use either of the following methods.
2. Manually, in the main program window by clicking **Install/Check** in **Update** > **Available version of ESET NOD32 Antivirus**.
3. Manually, by downloading and installing a new version over the previous one.
   At the beginning of installation, you can choose to preserve current program settings by selecting the **Use current settings** check box.

2.4 Entering username and password

For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct username and password are entered in the **Update setup**.

If you did not enter your username and password after the installation, you can do so now. From the main program window, click **Update**, then **Product activation...** and enter the license data you received with your ESET security product into the Product activation window.

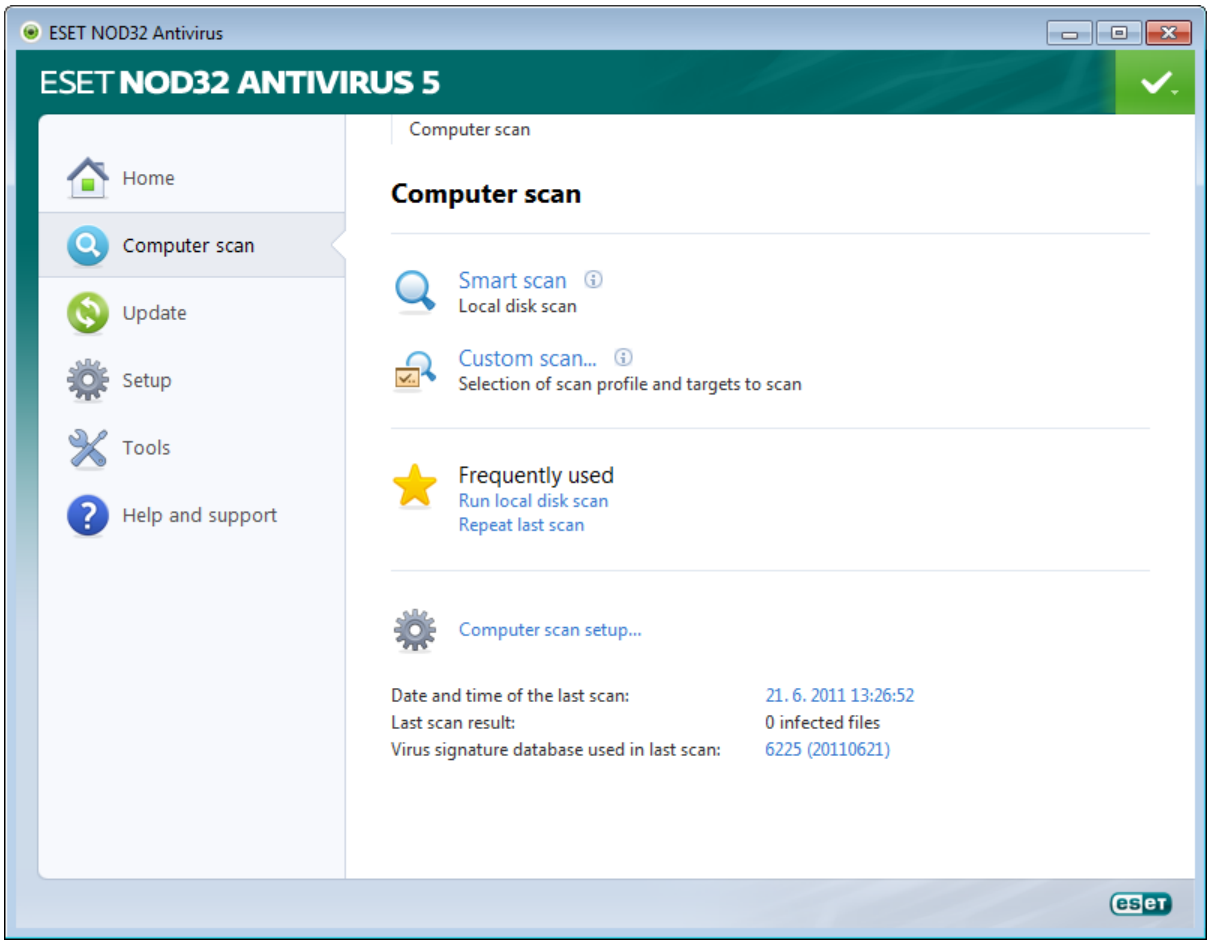
When typing your **Username** and **Password**, it is important to type them exactly as they are written:

- The username and password are case sensitive and the hyphen in the username is necessary.
- The password is ten characters long and all lowercase.
- We do not use the letter L in passwords (use the number one (1) instead).
- A big 'O' is the number zero (0), a little 'o' is the lowercase letter o.

We recommend copying and pasting the data from the registration email for maximum accuracy.

2.5 Computer scan

After installing ESET NOD32 Antivirus, you should perform a computer scan to check for malicious code. From the main program window, click **Computer scan** and then click **Smart scan**. For more information about computer scan, see section Computer scan.



3. Beginner's guide

This chapter provides an initial overview of ESET NOD32 Antivirus and its basic settings.

3.1 Introducing user interface design

The main program window of ESET NOD32 Antivirus is divided into two main sections. The primary window on the right displays information that corresponds to the option selected from the main menu on the left.

The following is a description of options within the main menu:

Home – Provides information about the protection status of ESET NOD32 Antivirus.

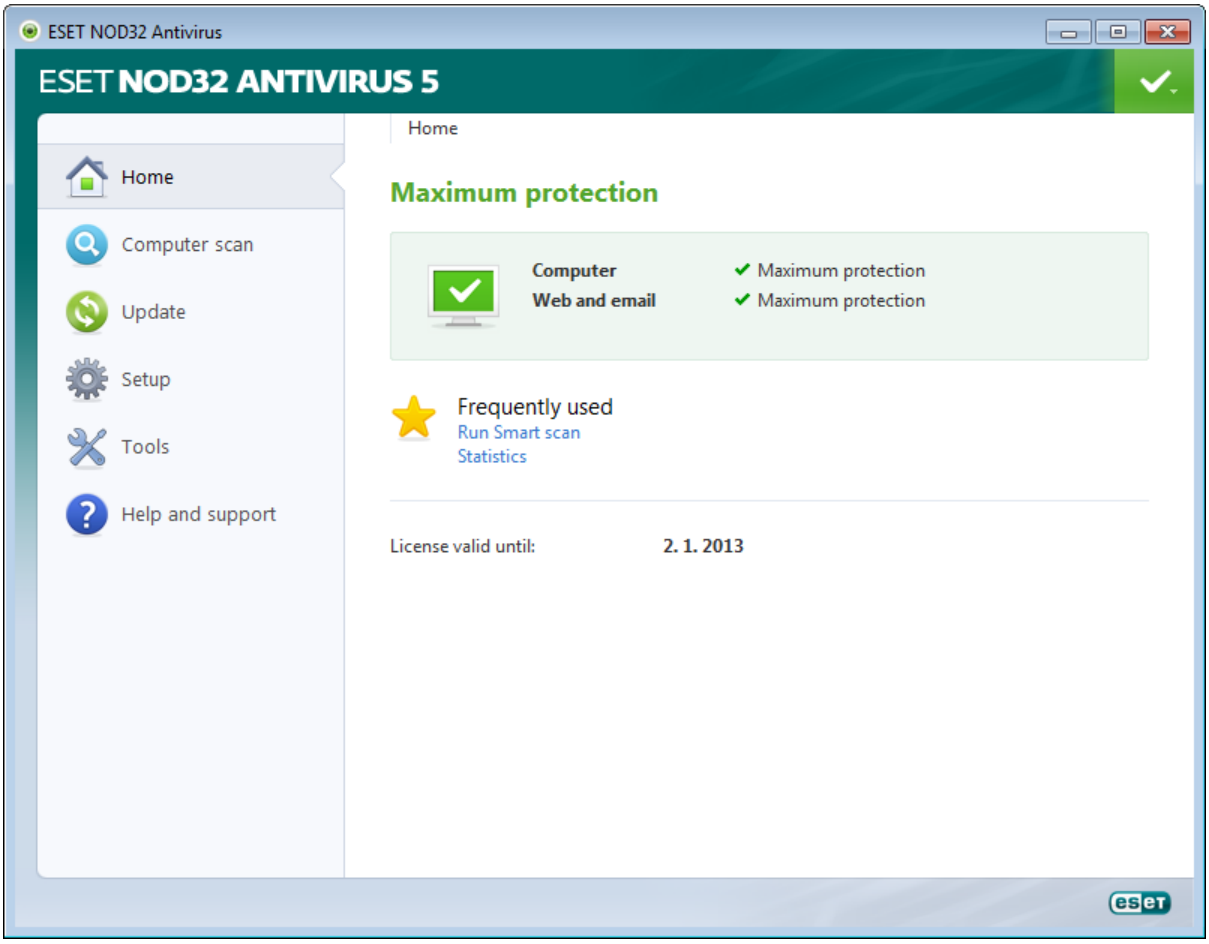
Computer scan – This option allows you to configure and launch a Smart scan or Custom scan.

Update – Displays information about updates to the virus signature database.

Setup – Select this option to adjust your security level for Computer, Web and Email.

Tools – Provides access to Log files, Protection statistics, Watch activity, Running processes, Scheduler, Quarantine, ESET SysInspector and ESET SysRescue.

Help and support – Provides access to help files, the ESET Knowledgebase, ESET's website and links to open a Customer Care support request.

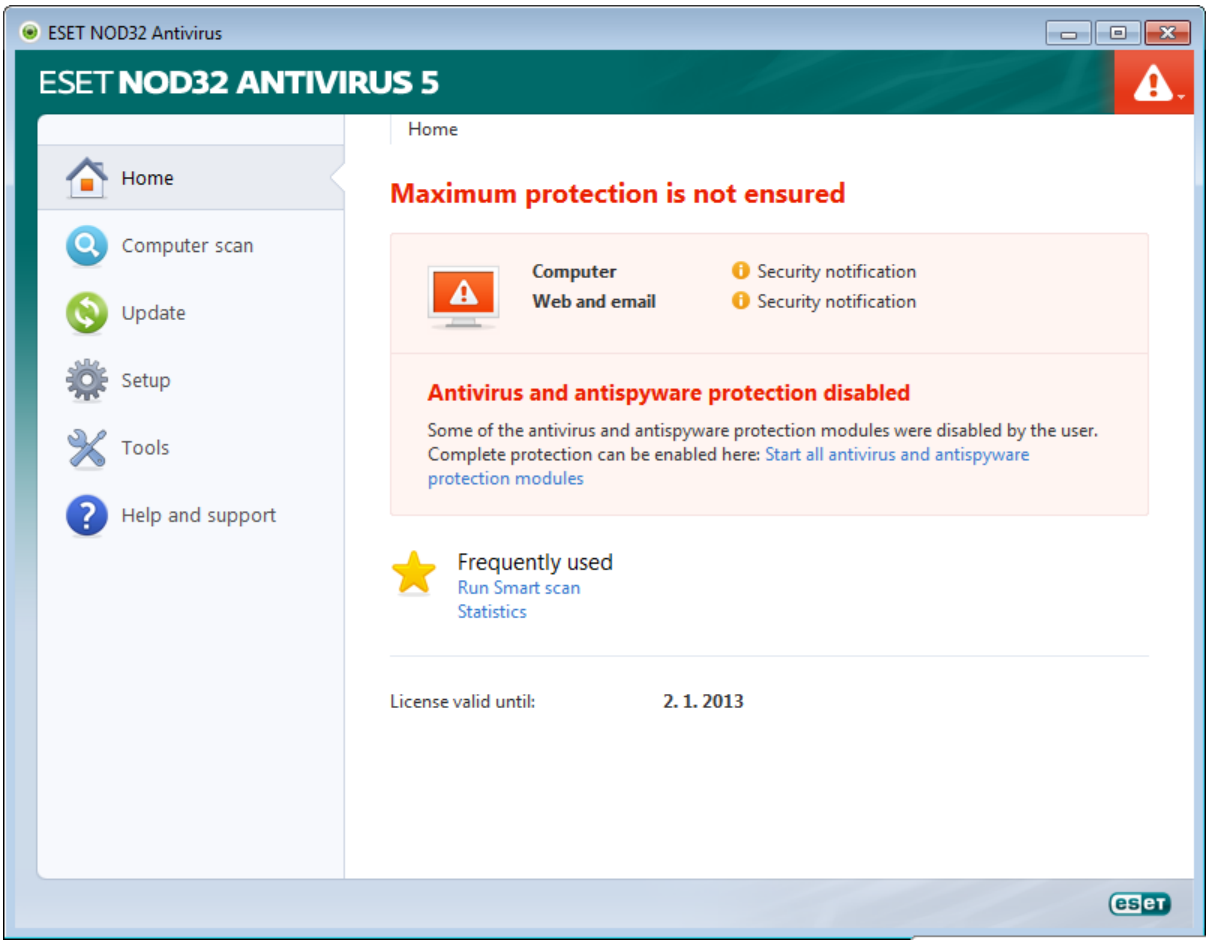


The **Home** screen informs you about the security and current protection level of your computer. The green **Maximum protection** status indicates that maximum protection is ensured.

The status window also displays frequently used features of ESET NOD32 Antivirus. Information about the program's expiration date can also be found here.

3.2 What to do if the program doesn't work properly

If the modules enabled are working properly, they are assigned a green check. If not, a red exclamation point or orange notification icon is displayed, and additional information about the module is shown in the upper part of the window. A suggested solution for fixing the module is also displayed. To change the status of individual modules, click **Setup** in the main menu and click on the desired module.



The red icon signals critical problems – maximum protection of your computer is not ensured. Possible reasons are:

- Disabled Real-time file system protection
- Outdated virus signature database
- Product not activated
- Product license is expired

The yellow icon indicates that Web access or Email client protection is disabled, there is a problem updating the program (outdated virus signature database, cannot update) or the license is nearing its expiration date.

Product not activated – This problem is signaled by a red warning and a security notification next to the **Computer** item. You can activate ESET NOD32 Antivirus from the program menu using the **Product activation...** option. The program menu is located in the right-top of the window.

Antivirus and antispyware protection disabled – This problem is signaled by a red display and a security notification next to the **Computer** item. You can re-enable antivirus protection by clicking on **Start all antivirus and antispyware protection modules**.

Your license will expire soon – This is indicated by the protection status icon is displaying an exclamation point. After the license expires, the program will not be able to update and the protection status icon will turn red.

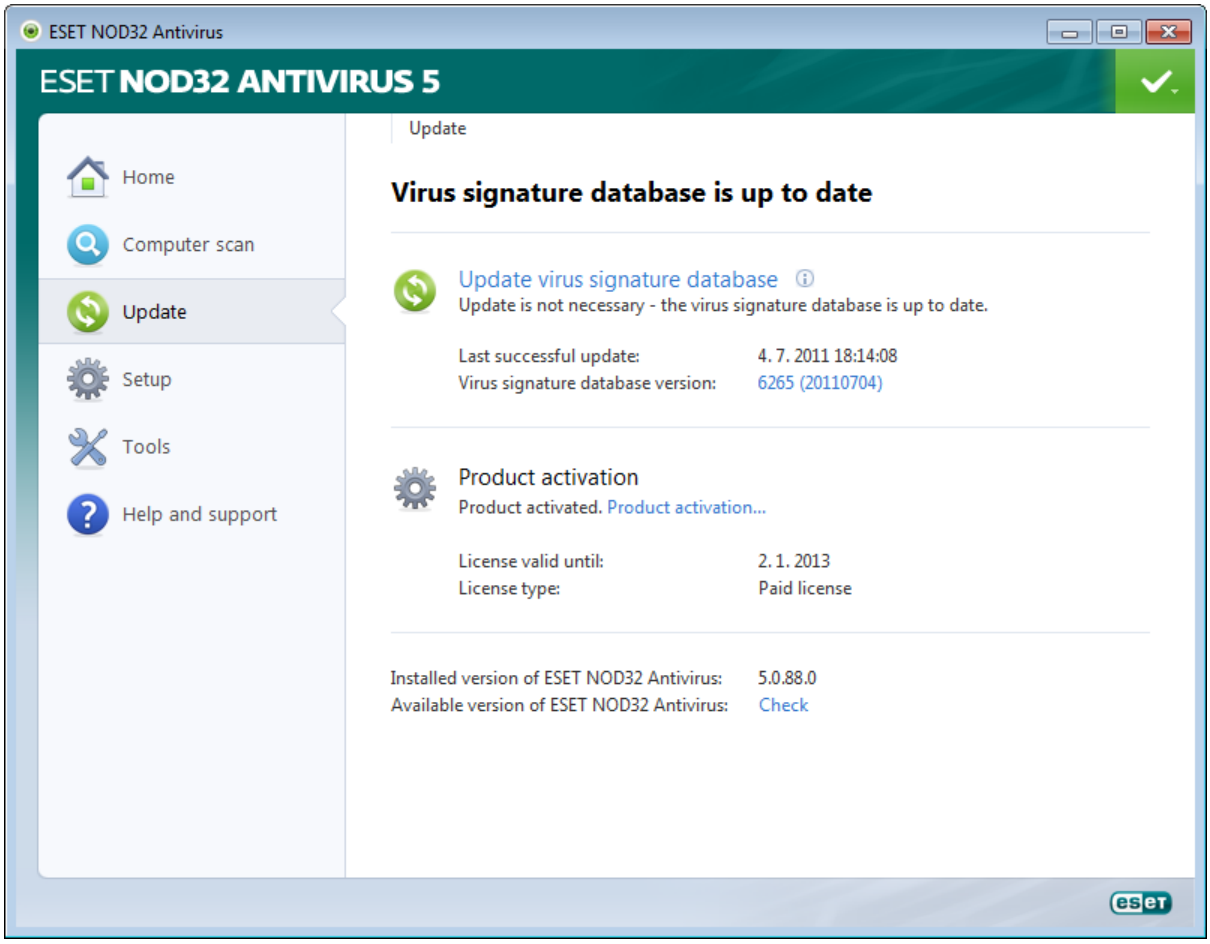
License expired – This is indicated by the protection status icon turning red. The program is not able to update from this time. We recommend following the instructions in the alert window to renew your license.

If you are unable to solve a problem using the suggested solutions, click **Help and support** to access the help files or search the knowledgebase. If you still need assistance, you can submit an ESET Customer Care support request. ESET Customer Care will respond quickly to your questions and help determine a resolution.

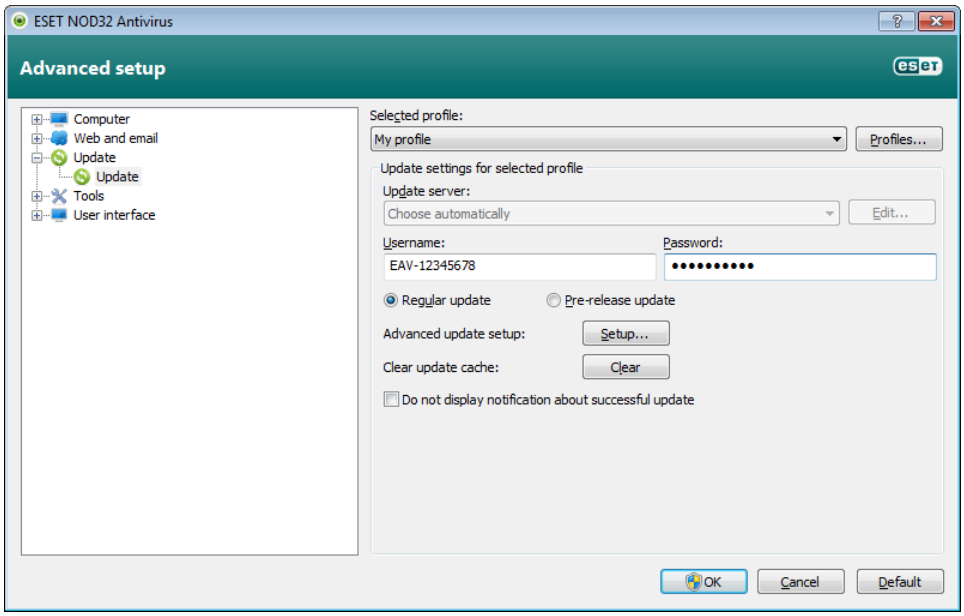
3.3 Update setup

Updating the virus signature database and updating program components are an important part of providing complete protection against malicious code. Please pay careful attention to their configuration and operation. From the main menu, select **Update** and then click **Update virus signature database** in the primary window to check for a newer database update.

If the username and password were not entered during installation or activation process of ESET NOD32 Antivirus you will be prompted for them at this point.

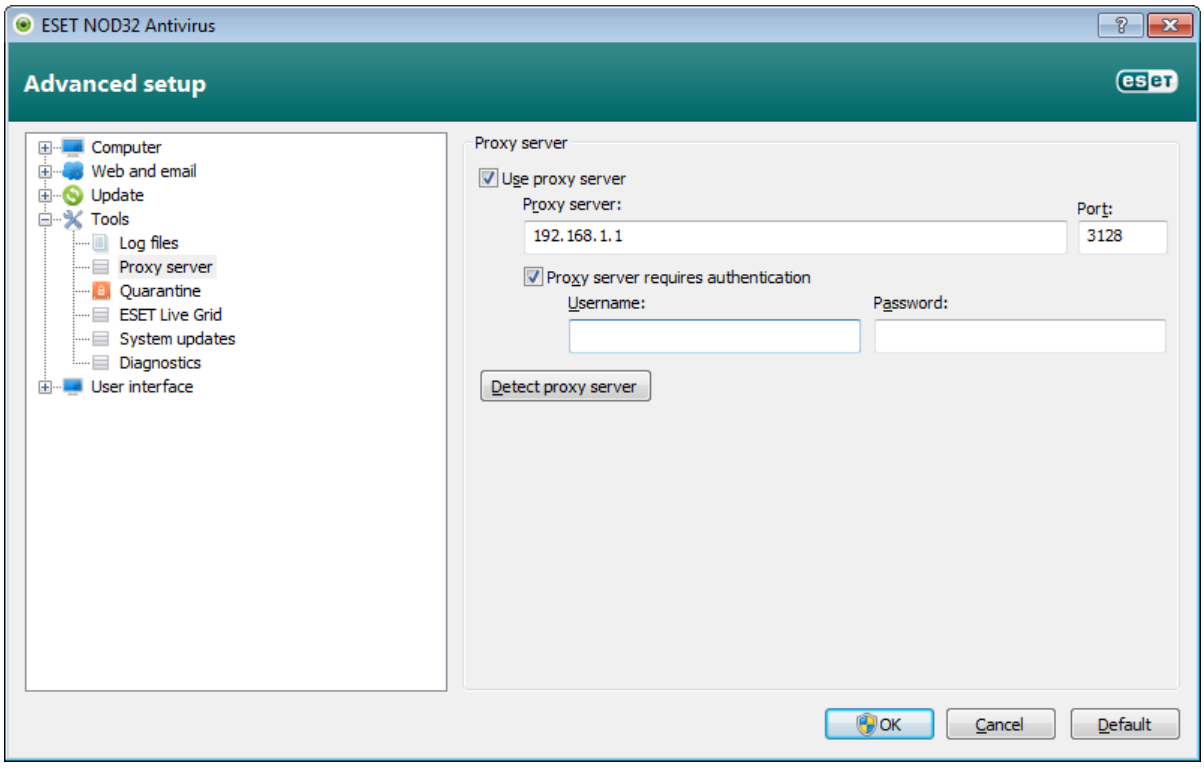

ESET NOD32 Antivirus
ESET NOD32 ANTIVIRUS 5
Home
Computer scan
Update
Setup
Tools
Help and support
Update
Virus signature database is up to date
Update virus signature database
Update is not necessary - the virus signature database is up to date.
Last successful update: 4. 7. 2011 18:14:08
Virus signature database version: 6265 (20110704)
Product activation
Product activated. Product activation...
License valid until: 2. 1. 2013
License type: Paid license
Installed version of ESET NOD32 Antivirus: 5.0.88.0
Available version of ESET NOD32 Antivirus: Check
eset

The Advanced setup window (click **Setup** from the main menu and then click **Enter advanced setup...**, or press F5 on your keyboard) contains additional update options. Click **Update** from the Advanced Setup tree on the left. The **Update server** drop-down menu should be set to **Choose automatically**. To configure advanced update options such as the update mode, proxy server access and LAN connections, click the **Setup...** button.



3.4 Proxy server setup

If you use a proxy server to control Internet connections on a system using ESET NOD32 Antivirus, it must be specified in Advanced Setup. To access the Proxy server configuration window, press F5 to open the Advanced Setup window and click **Tools** > **Proxy server** from the Advanced Setup tree. Select the **Use proxy server** option, and then fill in the **Proxy server** (IP address) and **Port** fields. If needed, select the **Proxy server requires authentication** option and then enter the **Username** and **Password**.

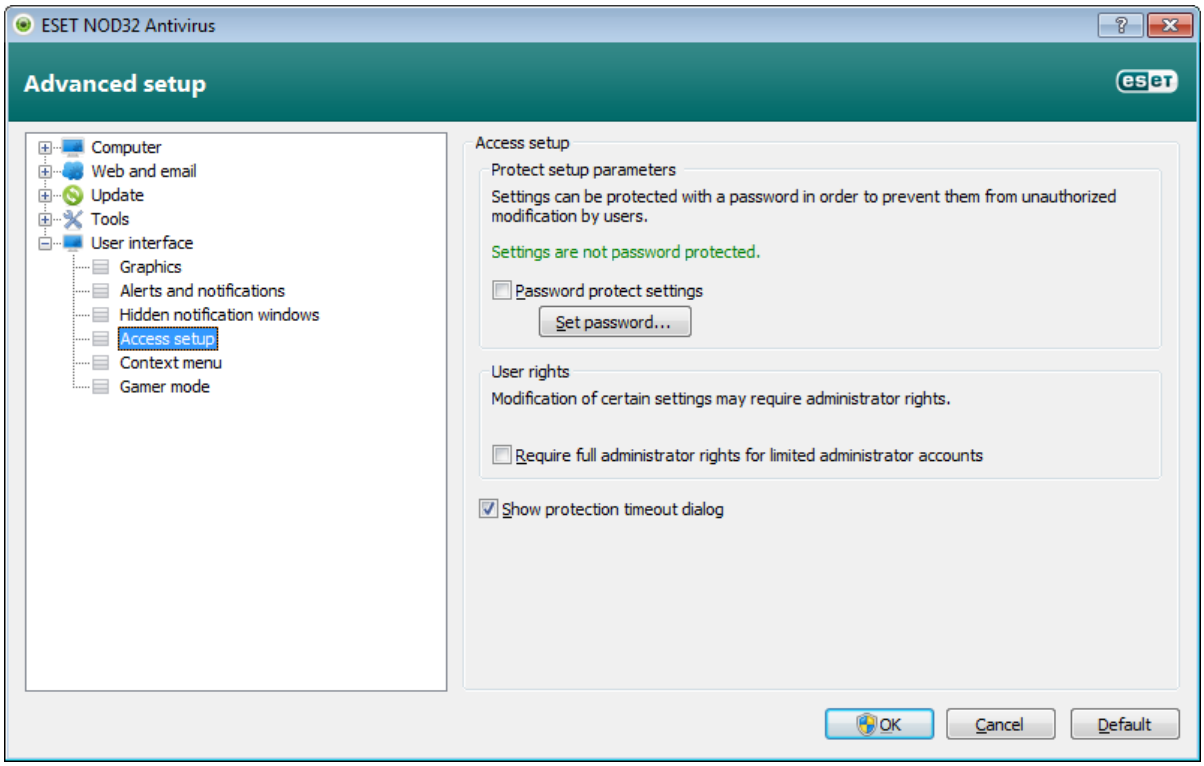


If this information is not available, you can try to automatically detect proxy server settings by clicking the **Detect proxy server** button.

NOTE: Proxy server options for various update profiles may differ. If this is the case, configure the different update profiles in Advanced Setup by clicking Update from the Advanced Setup tree.

3.5 Settings protection

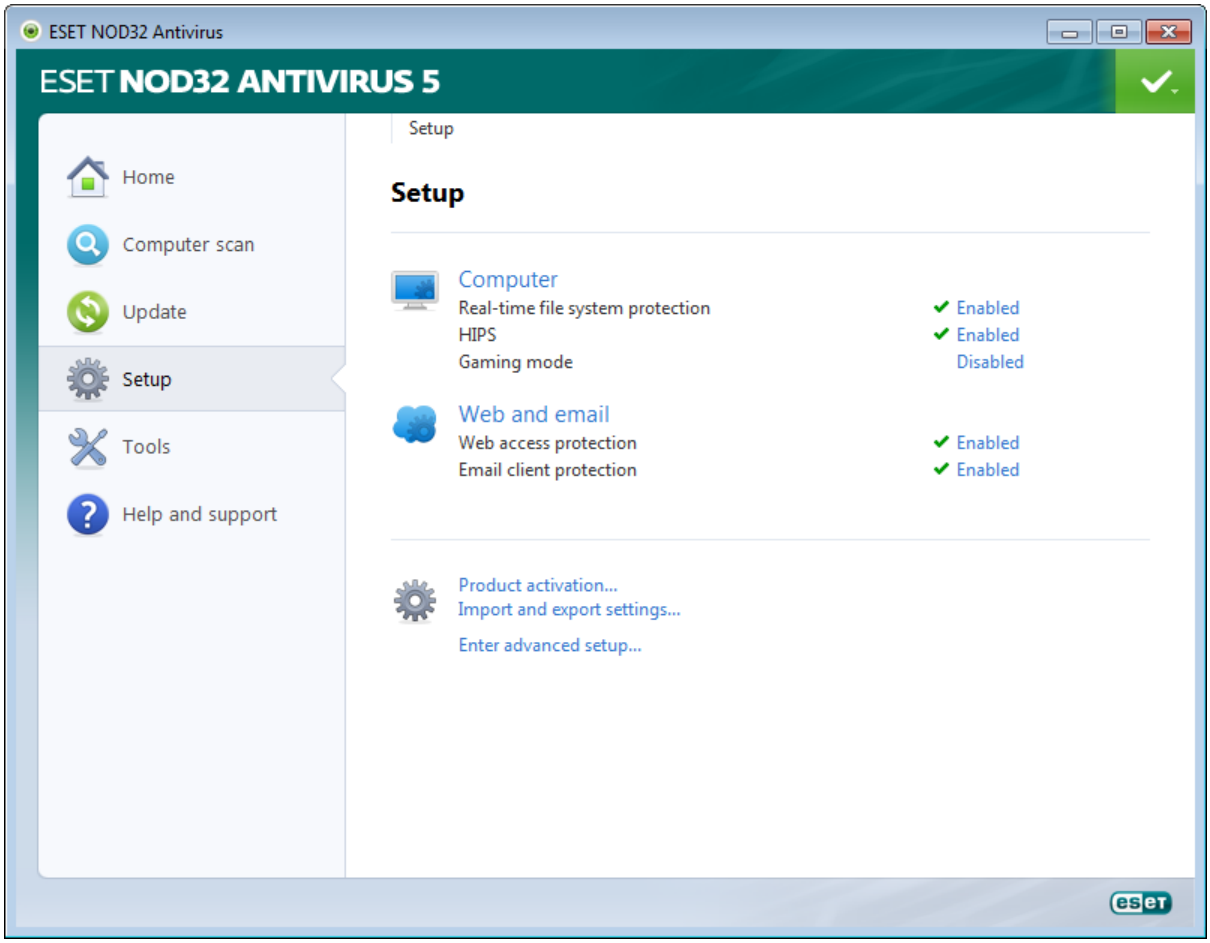
ESET NOD32 Antivirus settings can be very important from the perspective of your security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To password protect the setup parameters, from the main menu click **Setup** > **Enter advanced setup...** > **User interface** > **Access setup**, select the **Password protect settings** option and click the **Set password...** button.



Enter a password in the **New password** and **Confirm new password** fields and click **OK**. This password will be required for any future modifications to ESET NOD32 Antivirus.

4. Work with ESET NOD32 Antivirus

The ESET NOD32 Antivirus setup options allow you to adjust the protection levels of your computer.



The **Setup** menu contains following options:

- **Computer**
- **Web and Email**

Click any component to adjust the advanced settings of the corresponding protection module.

Computer protection setup allows you to enable or disable the following components:

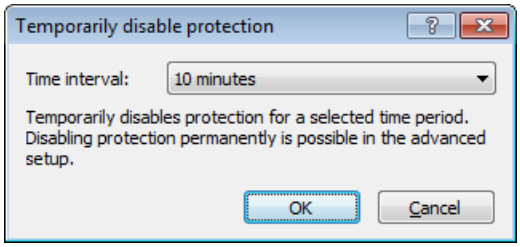
- **Real-time file system protection** – All files are scanned for malicious code when they are opened, created or run on your computer.
- **Document protection** – The document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements.
- **HIPS** – The HIPS system monitors the events within the operating system and reacts to them according to a customized set of rules.
- **Gamer mode** – Enables or disables the Gamer mode. You will receive a warning message (potential security risk) and the main window will turn yellow after enabling Gamer mode.

The **Web and Email** protection setup allows you to enable or disable the following components:

- **Web access protection** – If enabled, all traffic through HTTP or HTTPS is scanned for malicious software.
- **Email client protection** – Email protection provides control of email communication received through the POP3 and IMAP protocol.

NOTE: Document protection will display after enabling the option in **Enter advanced setup...** (F5) > **Computer** > **Antivirus and antispyware** > **Document protection** > **Integrate into system**.

After clicking **Enabled**, the **Temporary disable protection** dialog box will display. Click **OK** to disable the selected security component. A **Time interval** drop-down menu represents the period of time that the selected component will be disabled.


Temporarily disable protection
Time interval:
10 minutes
Temporarily disables protection for a selected time period. Disabling protection permanently is possible in the advanced setup.
OK
Cancel

To re-enable the protection of the disabled security component, click **Disabled**.

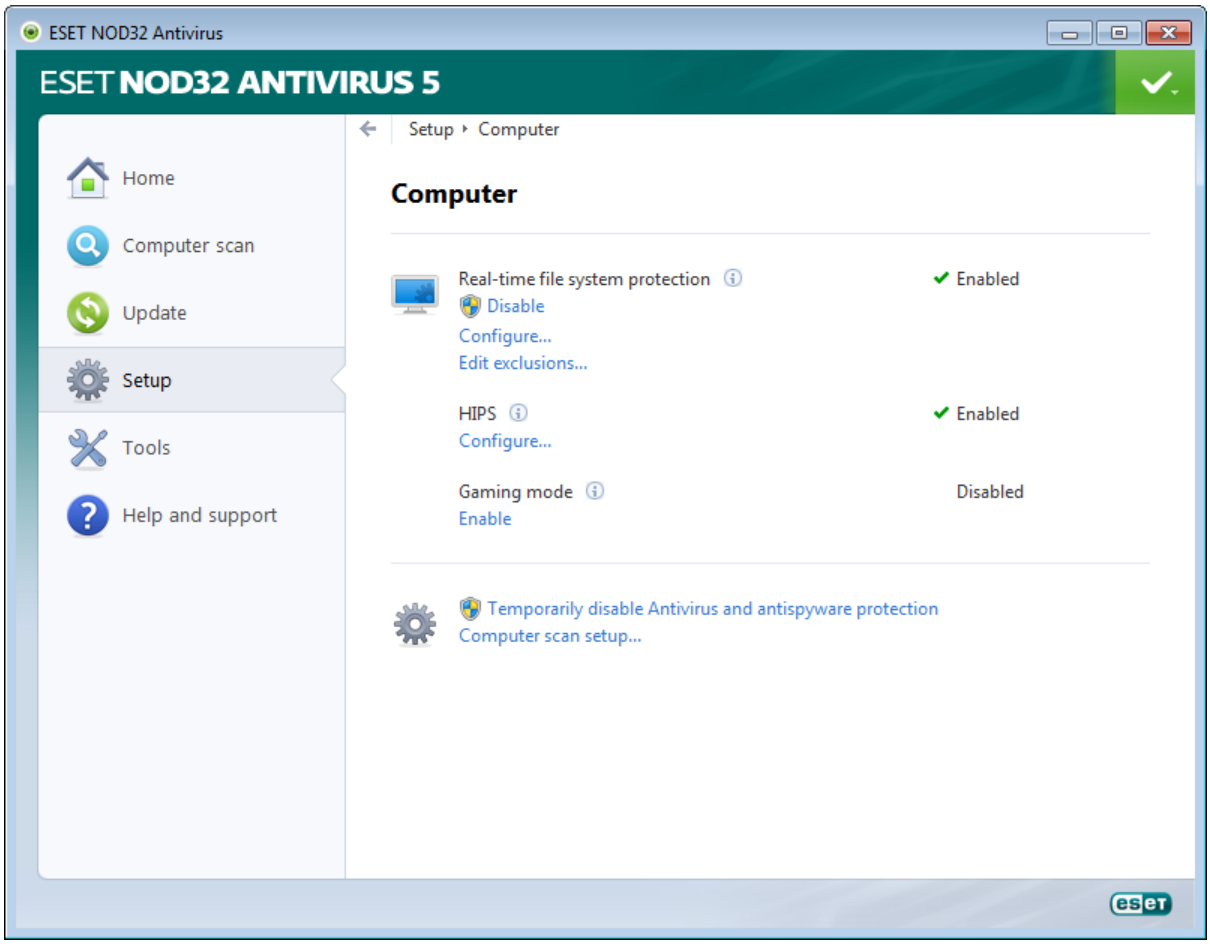
NOTE: When disabling protection using this method, all disabled parts of protection will be enabled after a computer restart.

There are additional options at the bottom of the setup window. Use the **Product activation...** link to open a registration form that will activate your ESET security product and send you an email with your authentication data (username and password). To load setup parameters using an *.xml* configuration file, or to save the current setup parameters to a configuration file, use the **Import and export settings...** option.

4.1 Computer

Computer configuration can be found in the **Setup** pane after clicking on the **Computer** title. It shows an overview of all protection modules. To turn off individual modules temporarily, click **Disable** below the desired module. Note that this may decrease the protection of your computer. To access detailed settings for each module, click **Configure...**.

Click **Edit exclusions...** to open the Exclusion setup window, which allows you to exclude files and folders from antivirus scanning.



Temporarily disable Antivirus and antispyware protection – Disables all antivirus and antispyware protection modules. **Temporary disable protection** dialog box with **Time interval** drop-down menu will display. A **Time interval** drop-down menu represents the period of time that the protection will be disabled. Click **OK** to confirm.

Computer scan setup... – Click to adjust the parameters of the on-demand scanner (manually executed scan).

4.1.1 Antivirus and antispyware protection

Antivirus and antispyware protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it, and then cleaning, deleting or moving it to quarantine.

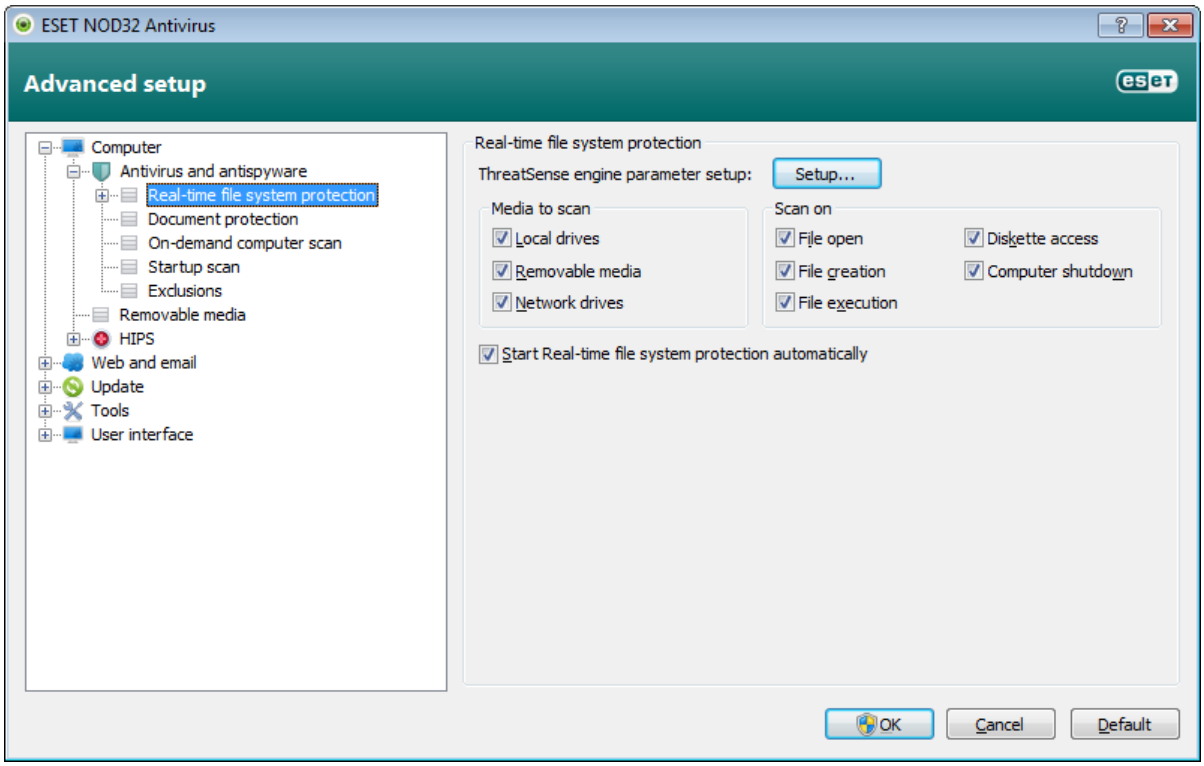
4.1.1.1 Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code at the moment they are opened, created or run on your computer. Real-time file system protection is launched at system startup.

The Real-time file system protection checks all types of media and is triggered by various system events such as accessing a file. Using ThreatSense technology detection methods (as described in section ThreatSense engine parameter setup), real-time file system protection may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.

To provide a minimal system footprint when using real-time protection, files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is configured using **Smart optimization**. If this is disabled, all files are scanned each time they are accessed. To modify this option, press F5 to open the Advanced Setup window and click **Computer** > **Antivirus and antispyware** > **Real-time file system protection** from the Advanced setup tree. Then click the **Setup...** button next to **ThreatSense engine parameter setup**, click **Other** and select or deselect the **Enable Smart optimization** option.

By default, Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another Real-time scanner), the real-time protection can be terminated by deselecting the **Start Real-time file system protection automatically** option.



4.1.1.1.1 Media to scan

By default, all types of media are scanned for potential threats.

Local drives – Controls all system hard drives.

Removable media – Diskettes, CD/DVDs, USB storage devices, etc.

Network drives – Scans all mapped drives.

We recommend that you keep the default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

4.1.1.1.2 Scan on (Event-triggered scanning)

By default, all files are scanned upon opening, creation or execution. We recommend that you keep the default settings, as these provide the maximum level of real-time protection for your computer.

File open – Enables or disables scanning of opened files.

File creation – Enables or disables scanning of newly created or modified files.

File execution – Enables or disables scanning of executed files.

Diskette access – Enables or disables scanning triggered by accessing the floppy drive.

Computer shutdown – Enables or disables control of the hard disk boot sectors during computer shutdown. Although boot viruses are rare today, we recommend that you leave these options enabled, as there is still the possibility of infection by a boot virus from alternate sources.

4.1.1.1.3 Advanced scan options

More detailed setup options can be found under **Computer** > **Antivirus and antispyware** > **Real-time system protection** > **Advanced setup**.

Additional ThreatSense parameters for newly created and modified files – The probability of infection in newly-created or modified files is comparatively higher than in existing files. For this reason, the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics are used, which greatly improves detection rates because heuristics can detect new threats before the virus signature database update is released. In addition to newly-created files, scanning is also performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, deselect the **Default archive scan settings** option.

Additional ThreatSense parameters for executed files – By default, advanced heuristics are not used when files are executed. However, in some cases you may want to enable this option (by checking the **Advanced heuristics on file execution** option). Note that advanced heuristics may slow the execution of some programs due to increased system requirements. While the **Advanced heuristics on executing files from removable media** option is enabled, if you wish to exclude some removable media (USB) ports from being scanned by advanced heuristics on file execution, click **Exceptions...** to open removable media drive exclusions window. From here, you can customize the settings by selecting or deselecting the checkboxes that represent each port.

4.1.1.1.4 Cleaning levels

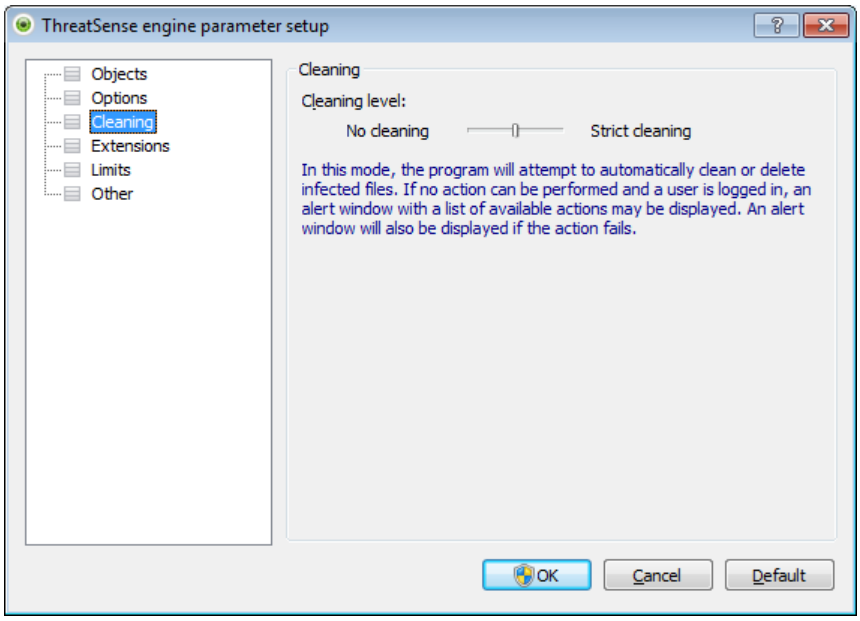
The real-time protection has three cleaning levels (to access, click the **Setup...** button in the **Real-time file system protection** section and then click the **Cleaning** branch).

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

Default level – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by an information message located in the bottom right corner of the screen. If it is not possible to select the correct action automatically, the program offers a selection of follow-up actions. The same happens if a predefined action couldn't be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

Warning: If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (**Default level**), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.


ThreatSense engine parameter setup
Objects
Options
Cleaning
Extensions
Limits
Other
Cleaning
Cleaning level:
No cleaning
Strict cleaning
In this mode, the program will attempt to automatically clean or delete infected files. If no action can be performed and a user is logged in, an alert window with a list of available actions may be displayed. An alert window will also be displayed if the action fails.
OK
Cancel
Default

4.1.1.1.5 When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Always be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases. For example, if there is a conflict with a certain application or real-time scanner of another antivirus program.

After installating ESET NOD32 Antivirus, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-right of the **Real-time file system protection** window (**Advanced Setup** > **Computer** > **Antivirus and antispyware** > **Real-time file system protection**).

4.1.1.1.6 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a special harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file eicar.com is available for download at http://www.eicar.org/download/eicar.com

4.1.1.1.7 What to do if real-time protection does not work

In this chapter, we describe problem situations that may arise when using real-time protection, and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** and click **Real-time file system protection** section of the main program window.

If real-time protection is not initiated at system startup, it is usually because the **Start Real-time file system protection automatically option** is disabled. To enable this option, navigate to Advanced Setup (F5) and click **Computer** > **Antivirus and antispyware** > **Real-time file system protection** in the Advanced Setup tree. In the **Advanced setup** section at the bottom of the window, make sure that the **Start Real-time file system protection automatically** checkbox is selected.

If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system.

Real-time protection does not start

If real-time protection is not initiated at system startup (and the **Start Real-time file system protection automatically** option is enabled), it may be due to conflicts with other programs. If this is the case, please consult ESET's Customer Care specialists.

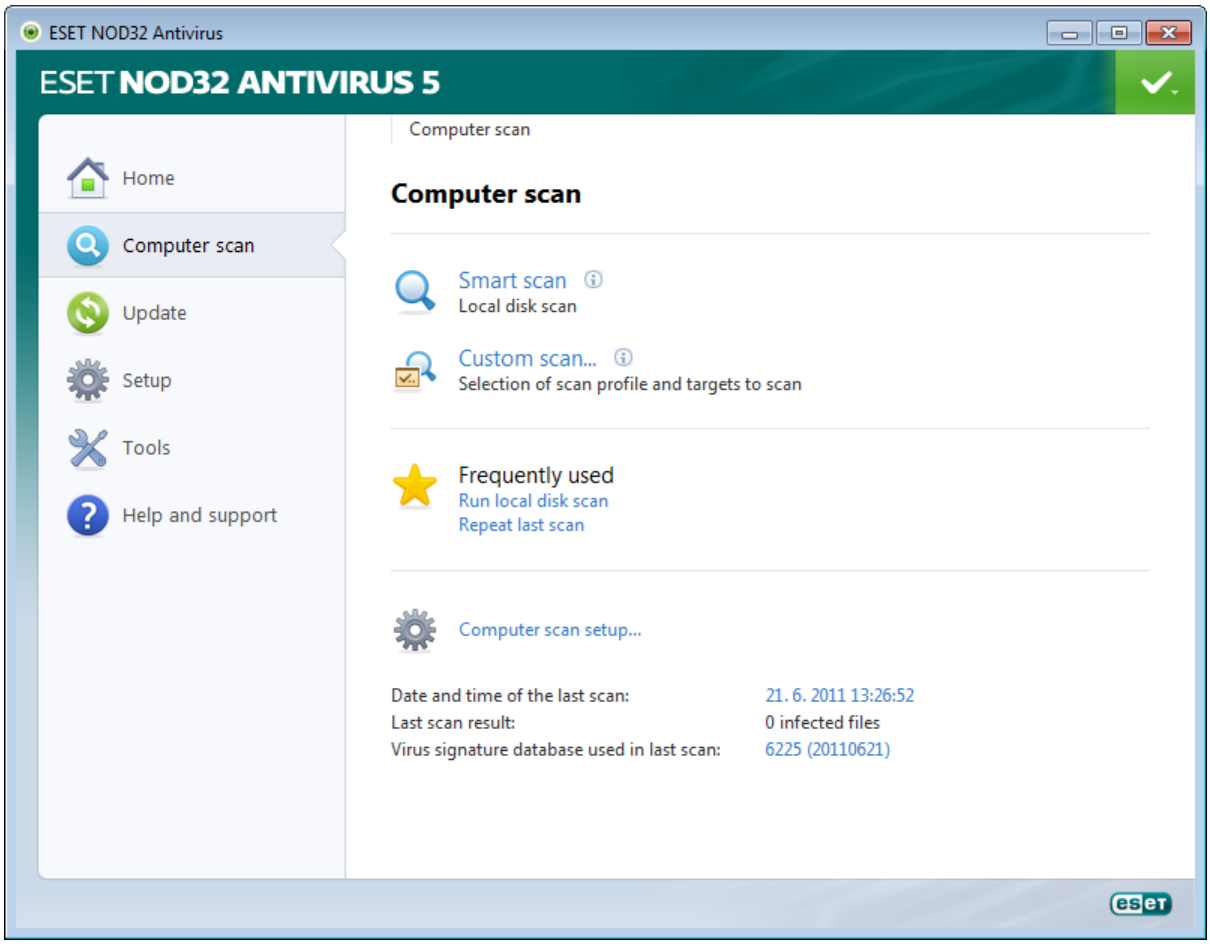
4.1.1.2 Document protection

The document protection feature scans Microsoft Office documents before they are opened, as well as files downloaded automatically by Internet Explorer, such as Microsoft ActiveX elements. The **Integrate into system** option activates the protection system. To modify this option, press F5 to open the Advanced Setup window and click **Computer** > **Antivirus and antispyware** > **Document protection** from the Advanced setup tree. When activated, the Document protection can be viewed from main window of ESET NOD32 Antivirus in **Setup** > **Computer**.

The feature is activated by applications which use the Microsoft Antivirus API (e.g., Microsoft Office 2000 and higher, or Microsoft Internet Explorer 5.0 and higher).

4.1.1.3 Computer scan

The on-demand scanner is an important part of your antivirus solution. It is used to perform scans of files and folders on your computer. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. We recommend that you perform regular in-depth scans of your system to detect possible viruses, which were not captured by the **Real-time file system protection** when they were written to disk.This can happen if the Real-time file system protection was disabled at the time, the virus database was obsolete or the file was not detected as virus when it was saved to the disk.



Two types of **Computer scan** are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan** allows you to select any of the predefined scan profiles, as well as choose specific scan targets.

See the Scan progress chapter for more information about the scanning process.

We recommend that you run a computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.

4.1.1.3.1 Type of scan

4.1.1.3.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. The advantage of Smart scan is it is easy to operate and does not require detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see section Cleaning.

4.1.1.3.1.2 Custom scan

Custom scan is an optimal solution if you wish to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. The configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and select an option from the **Scan targets** drop-down menu or select specific targets from the tree structure. A scan target can also be specified by entering the path to the folder or file(s) you wish to include. If you are only interested in scanning the system without additional cleaning actions, select the **Scan without cleaning** option. Furthermore, you can choose from three cleaning levels by clicking **Setup...** > **Cleaning**.

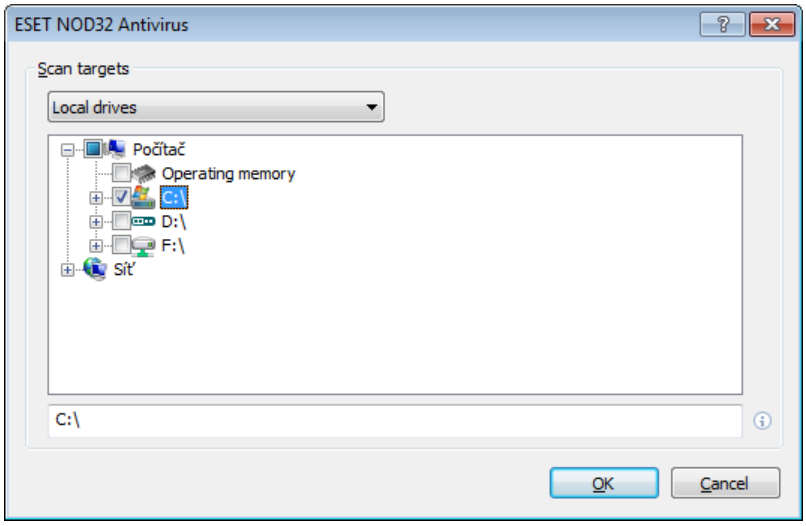
Performing computer scans with Custom scan is suitable for advanced users with previous experience using antivirus programs.

4.1.1.3.2 Scan targets

The Select scan targets window allows you to define which objects (memory, drives, sectors, files and folders) are scanned for infiltrations. The **Scan targets** drop-down menu allows you to select predefined scan targets.

- **By profile settings** – Selects targets set in the selected scan profile.
- **Removable media** – Selects diskettes, USB storage devices, CD/DVD.
- **Local drives** – Selects all system hard drives.
- **Network drives** – Selects all mapped network drives.
- **No selection** – Cancels all selections.

A scan target can also be specified by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure, which lists all devices available on the computer.



To quickly navigate to a scan target or to directly add a desired target, enter it in the blank field below the folder list. This is only possible, if no objects have been selected in the folder list. This is only possible if no targets were selected in the tree structure listing and the **Scan targets** menu is set to **No selection**.

4.1.1.3.3 Scan profiles

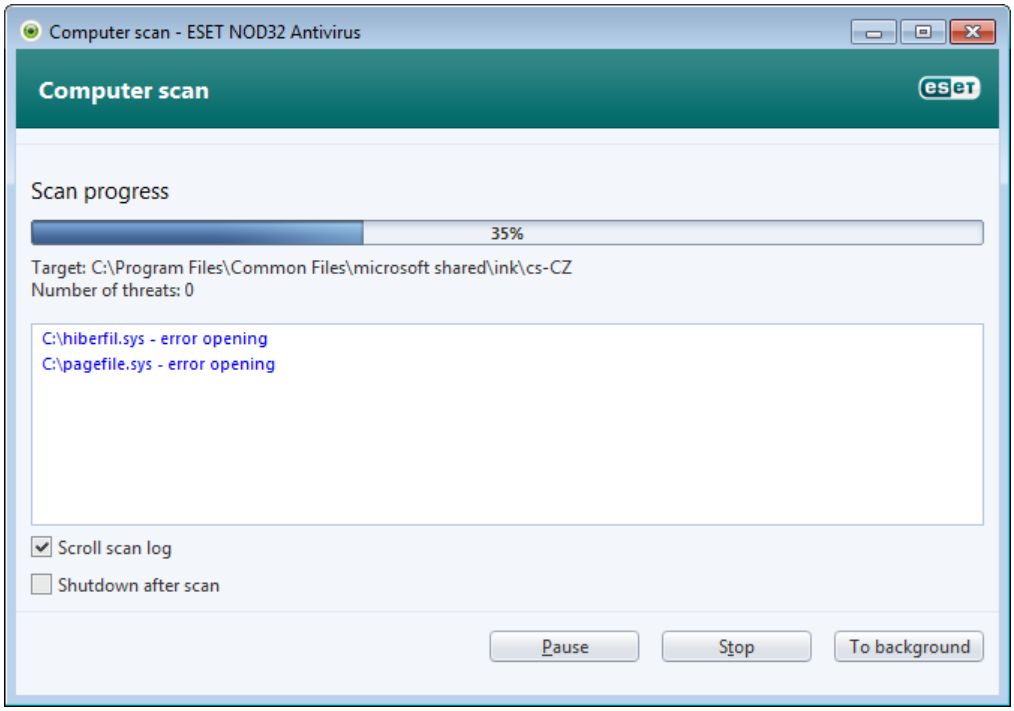
Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced Setup window (F5) and click **Computer scan** > **Profiles...** The **Configuration profiles** window has a drop-down menu of existing scan profiles and the option to create a new one. To help you create a scan profile to fit your needs, see section ThreatSense engine parameters setup for a description of each parameter of the scan setup.

Example: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. From the **Configuration profiles** window, click the **Add...** button. Enter the name of your new profile in the **Profile name** field, and select **Smart scan** from the **Copy settings from profile** drop-down menu. Then adjust the remaining parameters to meet your requirements.

4.1.1.3.4 Scan progress

The scan progress window shows the current status of the scan and information about the number of files found to contain malicious code.



NOTE: It is normal that some files, such as password protected files or files exclusively being used by the system (typically *pagefile.sys* and certain log files), cannot be scanned.

Scan progress – The progress bar shows the percentage of already-scanned objects compared to objects still waiting be scanned. The value is derived from the whole number of objects included in scanning.

Target – The name of the currently scanned object and its location.

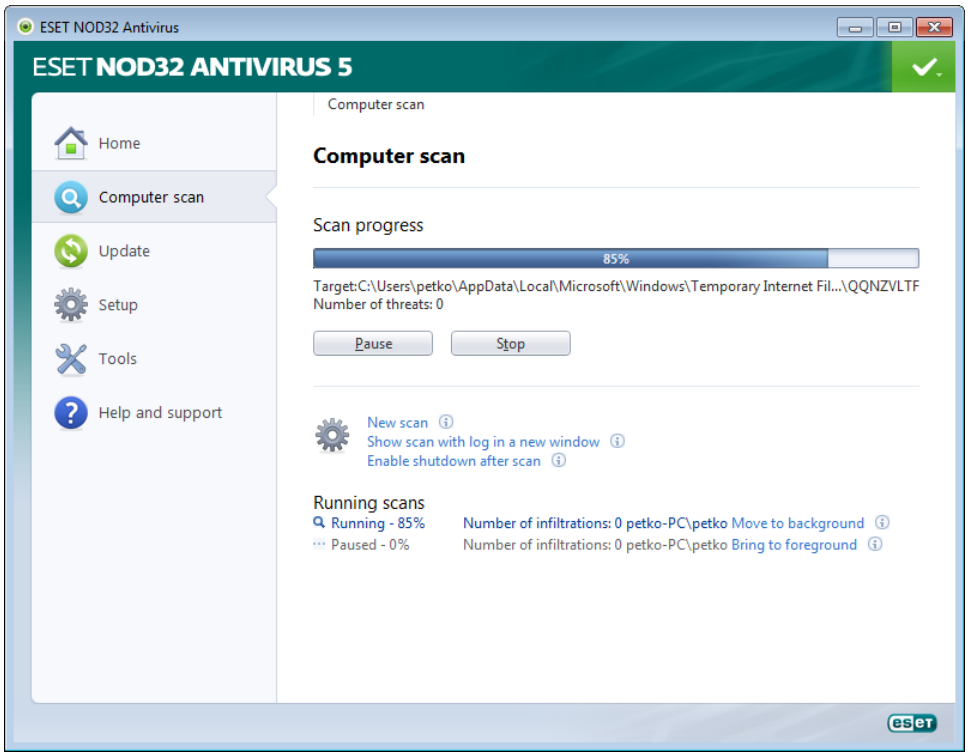
Number of threats – Shows the total number of threats found during the scan.

Pause – Pauses the scan.

Resume – This option is visible when scan progress was paused. Click **Resume** to continue scanning.

Stop – Terminates the scan.

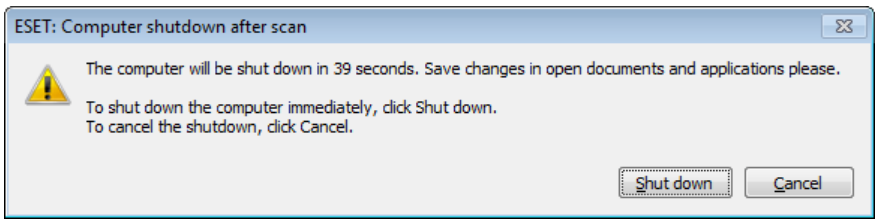
To background – You can run another parallel scan. The running scan will be minimized to the background.



Click **Bring to foreground** to return to the scanning process.

Scroll scan log – If enabled, the scan log will scroll down automatically as new entries are added so that the most recent entries are visible.

Enable shutdown after scan – Enables a scheduled shutdown when the on-demand computer scan finishes. A confirmation shutdown dialog window will open with a 60 second timeout. Click **Cancel** if you wish to deactivate the requested shutdown.

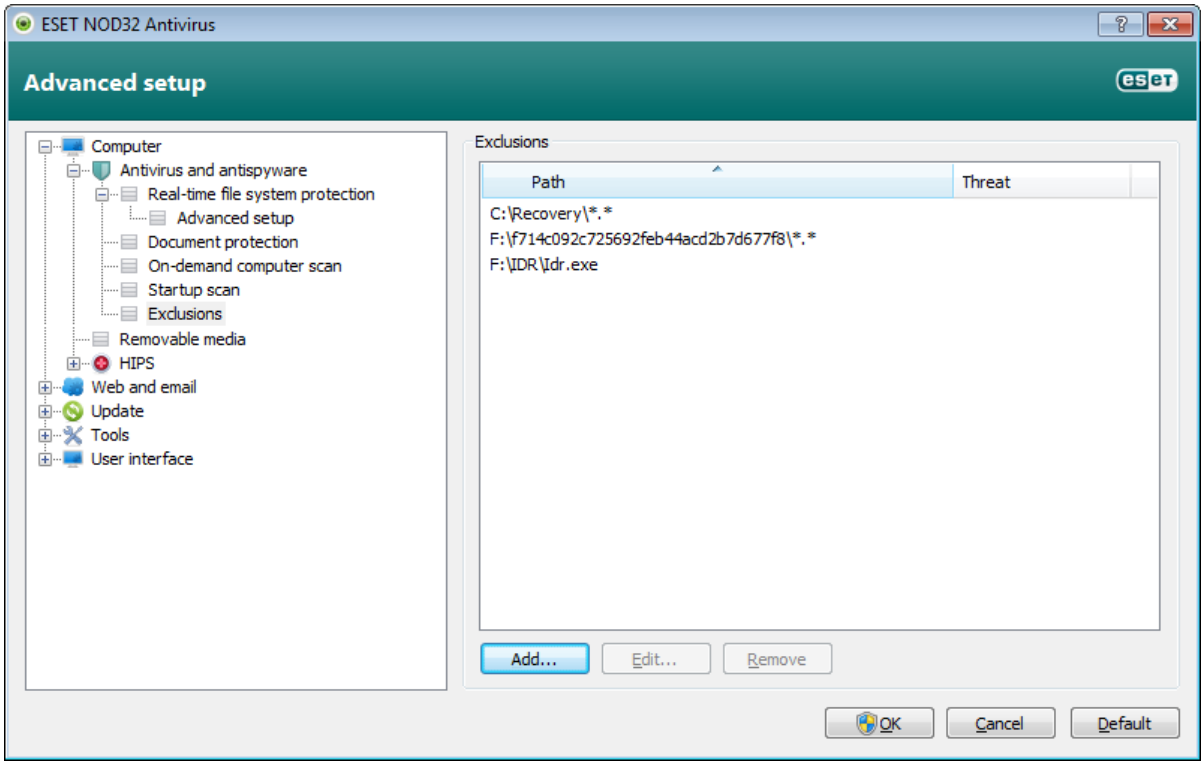

ESET: Computer shutdown after scan
The computer will be shut down in 39 seconds. Save changes in open documents and applications please.
To shut down the computer immediately, click Shut down.
To cancel the shutdown, click Cancel.
Shut down
Cancel

4.1.1.4 Startup scan

When the Real-time file system protection is enabled, the automatic startup file check will be performed on system startup or virus signature database update. This scan is dependent upon the **Scheduler** configuration and tasks.

4.1.1.5 Exclusions

Exclusions enable you to exclude files and folders from scanning. We do not recommend that you alter these options, to ensure that all objects are scanned for threats. However, there are cases you may need to exclude an object. For example, large database entries that would slow down the computer during the scan or software that has conflicts with the scan.



Path – Path to excluded files and folders.

Threat – If there is a name of a threat next to an excluded file, it means that the file is only excluded for the given threat, not completely. Therefore if that file becomes infected later with other malware, it will be detected by the antivirus module. This type of exclusion can only be used for certain types of infiltrations and it can be created either in the threat alert window reporting the infiltration (click **Show advanced options** and then select **Exclude from detection**), or in **Setup** > **Quarantine** using the context menu option **Restore and exclude from detection** on the quarantined file.

Add... – Excludes objects from detection.

Edit... – Enables you to edit selected entries.

Remove – Removes selected entries.

To exclude an object from scanning:

1. Select **Add...**,
2. Enter the path to an object or select it in the tree structure below.

When configuring exclusions, special symbols – wildcards, such as "*" and "?" can be used.

Examples

- If you wish to exclude all files in a folder, type the path to the folder and use the mask "*.*".
- If you want to exclude doc files only, use the mask "*.doc".
- If the name of an executable file has a certain number of characters (and characters vary) and you only know the first one for sure (say "D"), use the following format: "D????.exe". Question marks replace the missing (unknown) characters.

4.1.1.6 ThreatSense engine parameters setup

ThreatSense is technology consists of many complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, virus signatures) which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

The ThreatSense technology setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned,
- The combination of various detection methods,
- Levels of cleaning, etc.

To enter the setup window, click the **Setup...** button located in any module's setup window which uses ThreatSense technology (see below). Different security scenarios could require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection,
- Document protection,
- Email client protection,
- Web access protection,
- and Computer scan.

The ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). We recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

4.1.1.6.1 Objects

The **Objects** section allows you to define which computer components and files will be scanned for infiltrations.

Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors – Scans boot sectors for the presence of viruses in the master boot record.

Email files – The program supports the following extensions: DBX (Outlook Express) and EML.

Archives – The program supports the following extensions: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE, and many others.

Self-extracting archives – Self-extracting archives (SFX) are archives needing no specialized programs – archives – to decompress themselves.

Runtime packers – After executing, runtime packers (unlike standard archive types) decompress in memory. In addition to standard static packers (UPX, yoda, ASPack, FSG, etc.), the scanner supports (thanks to code emulation) many more types of packers.

4.1.1.6.2 Options

Use the **Options** section to select the methods used when scanning the system for infiltrations. The following options are available:

Heuristics – A heuristic is an algorithm analyzing the (malicious) activity of programs. The main advantage is the ability to identify malicious software which did not exist, or was not known by the previous virus signatures database. The disadvantage is a (very small) probability of false alarms.

Advanced heuristics/DNA/Smart signatures – Advanced heuristics consist of a unique heuristic algorithm developed by ESET, optimized for detecting computer worms and trojan horses and written in high level programming languages. Thanks to advanced heuristics, the detecting capabilities of the program are significantly higher. Signatures can reliably detect and identify viruses. Utilizing the automatic update system, new signatures are available within a few hours of a threat discovery. The disadvantage of signatures is that they only detect viruses they know (or their slightly modified versions).

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously (pop-ups, ads),
- Activating and running of hidden processes,
- Increased usage of system resources,
- Changes in search results,
- Application communicates with remote servers.

Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, password-cracking applications, and keyloggers (programs recording each keystroke typed by a user). This option is disabled by default.

ESET Live Grid – Thanks to ESET's reputation technology, information about scanned files is verified against data from cloud-based ESET Live Grid to improve detection and scanning speed.

4.1.1.6.3 Cleaning

The cleaning settings determine the behavior of the scanner while cleaning infected files. There are 3 levels of cleaning:

No cleaning – Infected files will not be cleaned automatically. The program will display a warning window and allow the user to choose an action. This level is designed for more advanced users who know which steps to take in the event of an infiltration.

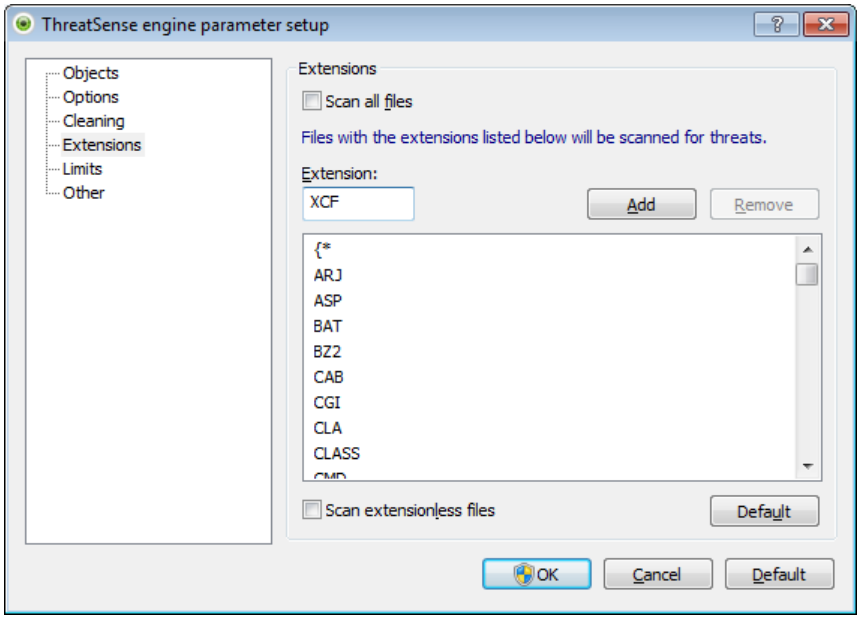
Default level – The program will attempt to automatically clean or delete an infected file based on a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by an information message located in the bottom right corner of the screen. If it is not possible to select the correct action automatically, the program offers a selection of follow-up actions. The same happens if a predefined action couldn't be completed.

Strict cleaning – The program will clean or delete all infected files. The only exceptions are the system files. If it is not possible to clean them, the user is prompted to select an action by a warning window.

Warning: If an archive contains a file or files which are infected, there are two options for dealing with the archive. In standard mode (**Default level**), the whole archive would be deleted if all the files it contains are infected files. In **Strict cleaning** mode, the archive would be deleted if it contains at least one infected file, regardless of the status of the other files in the archive.

4.1.1.6.4 Extension

An extension is a part of a file name delimited by a period. An extension defines the type and content of a file. This section of the ThreatSense parameter setup lets you define the types of files to scan.



By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. If the **Scan all files** option is deselected, the list changes to show all currently scanned file extensions.

To enable scanning files without an extension, select the **Scan extensionless files** option. The **Do not scan extensionless files** option becomes available when the **Scan all files** option is enabled.

Excluding files is sometimes necessary if scanning certain file types prevents the program which is using the extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

Using the **Add** and **Remove** buttons, you can allow or prohibit scanning of specific file extensions. Typing an **Extension** activates the **Add** button, which adds the new extension to the list. Click an extension in the list and then click the **Remove** button to delete that extension from the list.

The special symbols * (asterisk) and ? (question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list.

To scan the default set of extensions only, click on the **Default** button and confirm.

4.1.1.6.5 Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Maximum object size – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. This option should only be changed by advanced users who may have specific reasons for excluding larger objects from scanning. Default value: *unlimited*.

Maximum scan time for object (sec.) – Defines the maximum time value for scanning of an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished. Default value: *unlimited*.

Archive nesting level – Specifies the maximum depth of archive scanning. Default value: *10*.

Maximum size of file in archive – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. Default value: *unlimited*.

If scanning of an archive is prematurely terminated for these reasons, the archive checkbox will remain unchecked.

Note: We do not recommend changing the default values; under normal circumstances, there should be no reason to modify them.

4.1.1.6.6 Other

You can configure the following options in the **Other** section:

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected. For example, if an infiltration is found within an archive, the log will list also clean files contained within the archive.

Enable Smart optimization – With Smart Optimization enabled, the most optimal settings are used to ensure the most efficient scanning level, while simultaneously maintaining the highest scanning speeds. The various protection modules scan intelligently, making use of different scanning methods and applying them to specific file types. If the Smart Optimization is disabled, only the user-defined settings in the ThreatSense core of the particular modules are applied when performing a scan.

When configuring an Computer scan ThreatSense engine parameters setup, there are also the following options:

Scan alternate data streams (ADS) – Alternate data streams used by the NTFS file system are file and folder associations which are invisible by ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternate data streams.

Run background scans with low priority – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Preserve last access timestamp – Select this option to keep the original access time of scanned files instead of updating them (e.g., for use with data backup systems).

Scroll scan log – This option allows you to enable/disable log scrolling. If selected, information scrolls upwards within the display window.

4.1.1.7 An infiltration is detected

Infiltrations can reach the system from various entry points, such as webpages, shared folders, via email or from removable computer devices (USB, external disks, CDs, DVDs, diskettes, etc.).

If your computer is showing signs of a malware infection, e.g., it is slower, often freezes, etc., we recommend that you do the following:

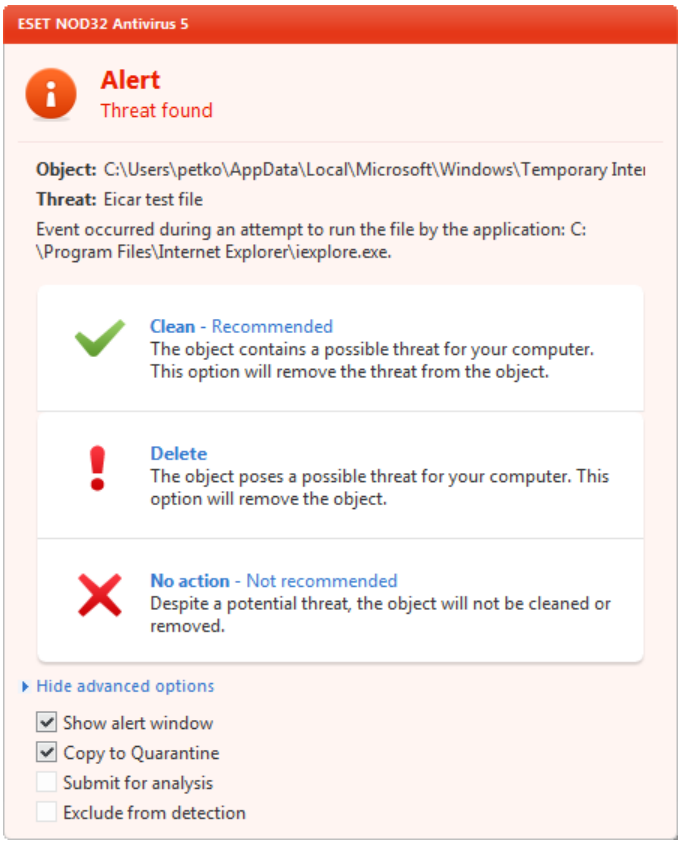
- Open ESET NOD32 Antivirus and click Computer scan,
- Click **Smart scan** (for more information, see section Smart scan),
- After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only wish to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

As a general example of how infiltrations are handled in ESET NOD32 Antivirus, suppose that an infiltration is detected by the real-time file system protection, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no predefined action to take for the real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **No action** are available. Selecting **No action** is not recommended, since the infected file(s) would be left untouched. The exception to this is when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting

Apply cleaning if a file has been attacked by a virus which has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.


ESET NOD32 Antivirus 5
Alert
Threat found
Object: C:\Users\petko\AppData\Local\Microsoft\Windows\Temporary Inte
Threat: Eicar test file
Event occurred during an attempt to run the file by the application: C:\Program Files\Internet Explorer\iexplore.exe.
Clean - Recommended
The object contains a possible threat for your computer. This option will remove the threat from the object.
Delete
The object poses a possible threat for your computer. This option will remove the object.
No action - Not recommended
Despite a potential threat, the object will not be cleaned or removed.
Hide advanced options
Show alert window
Copy to Quarantine
Submit for analysis
Exclude from detection

If an infected file is "locked" or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Deleting files in archives

In Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. However, use caution when performing a Strict cleaning scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

4.1.2 Removable media scanning and blocking

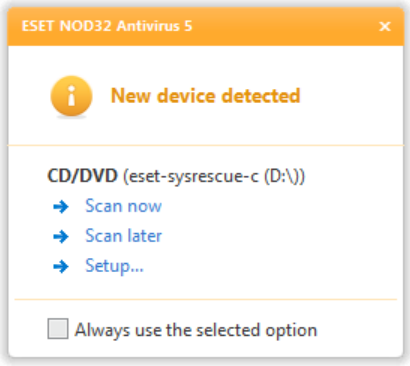
ESET NOD32 Antivirus provides automatic removable media (CD/DVD/USB/...) control. This module allows you to scan, block or adjust extended filters/permissions and select how the user can access and work with a given device. This may be useful if the computer administrator wishes to prevent removable media insertion with unsolicited content by users.

Supported removable media

- CD/DVD/Blu-ray
- USB key
- USB drive
- FireWire

Action to take after inserting removable media – Select the default action that will be performed when a removable media device is inserted into the computer (CD/DVD/USB). If the **Show scan options** option is selected, a notification will display which allows you to choose a desired action:

- **Scan now** – An on-demand computer scan of the inserted removable media device will be performed.
- **Scan later** – No action will be performed and the **New device detected** window will be closed.
- **Setup...** – Opens the Removable media setup section.



Removable media blocking rules – Select this option to block all removable media connected to the computer. If you wish some media to be available, then exclude it from blocking.

Click **Rules...** to allow or block access to selected removable media. You can manage extended rules for removable media in this window. Rules can be filtered for example by media size, serial number and device type. Each rule has its own permissions, so you can allow, limit or block access to the selected removable media.

4.1.3 Host-based Intrusion Prevention System (HIPS)

Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting to negatively affect your computer. HIPS utilizes advanced behavioral analysis coupled with the detection capabilities of network filtering to monitor running processes, files and registry keys, actively blocking and preventing any such attempts.

HIPS can be found in **Advanced Setup** (F5) by clicking on **Computer** > **HIPS**. The HIPS state (enabled/disabled) is shown in the ESET NOD32 Antivirus main window, in the **Setup** pane, on the right side of the **Computer** section.

Warning: Changes to the HIPS settings should only be made by an experienced user.

ESET NOD32 Antivirus has a built-in *Self-defense* technology that prevents malicious software from corrupting or disabling your antivirus and antispyware protection, so you can be sure your system is protected all the times. Changes to the **Enable HIPS** and **Enable Self-defense** settings take effect after the Windows operating system is restarted. Disabling the entire **HIPS** system will also require a computer restart. Filtering can be performed in one of four modes:

Automatic mode with rules – Operations are enabled, except pre-defined rules that protect your system.

Interactive mode – User will be prompted to confirm operations.

Policy-based mode – Operations are blocked.

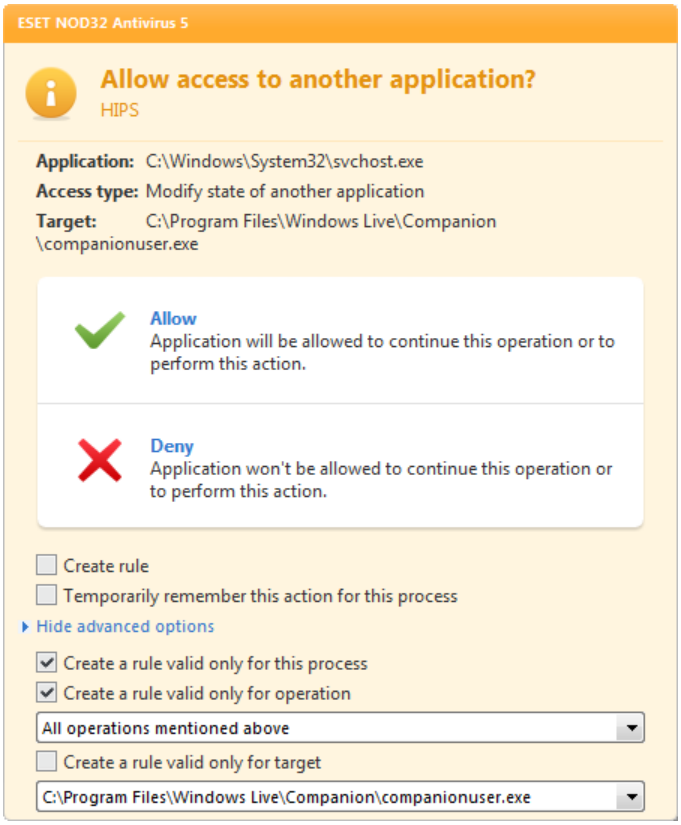
Learning mode – Operations are enabled and a rule is created after each operation. Rules created in this mode can be viewed in the **Rule editor**, but their priority is lower that the priority of the rules created manually or rules created in the automatic mode. After selecting **Learning mode**, the option **Notify about learning mode expiration in X days** becomes clickable. After that time period is over, learning mode is disabled again. The maximum time period is 14 days.

After this time period is over, a pop-up window will open in which you can edit the rules and select a different filtering mode.

The HIPS system monitors events inside the operating system and reacts accordingly based on the rules, which are similar to the rules from the personal firewall.

Click **Configure rules...** to open the HIPS rule management window, where the rules are stored and you can select, create,edit or delete them.

A dialog window is shown every time if **Ask** is the default action. It allows the user to choose to **Deny** or **Allow** the operation. If the user does not choose an action in the given time, a new action is selected based on the rules.

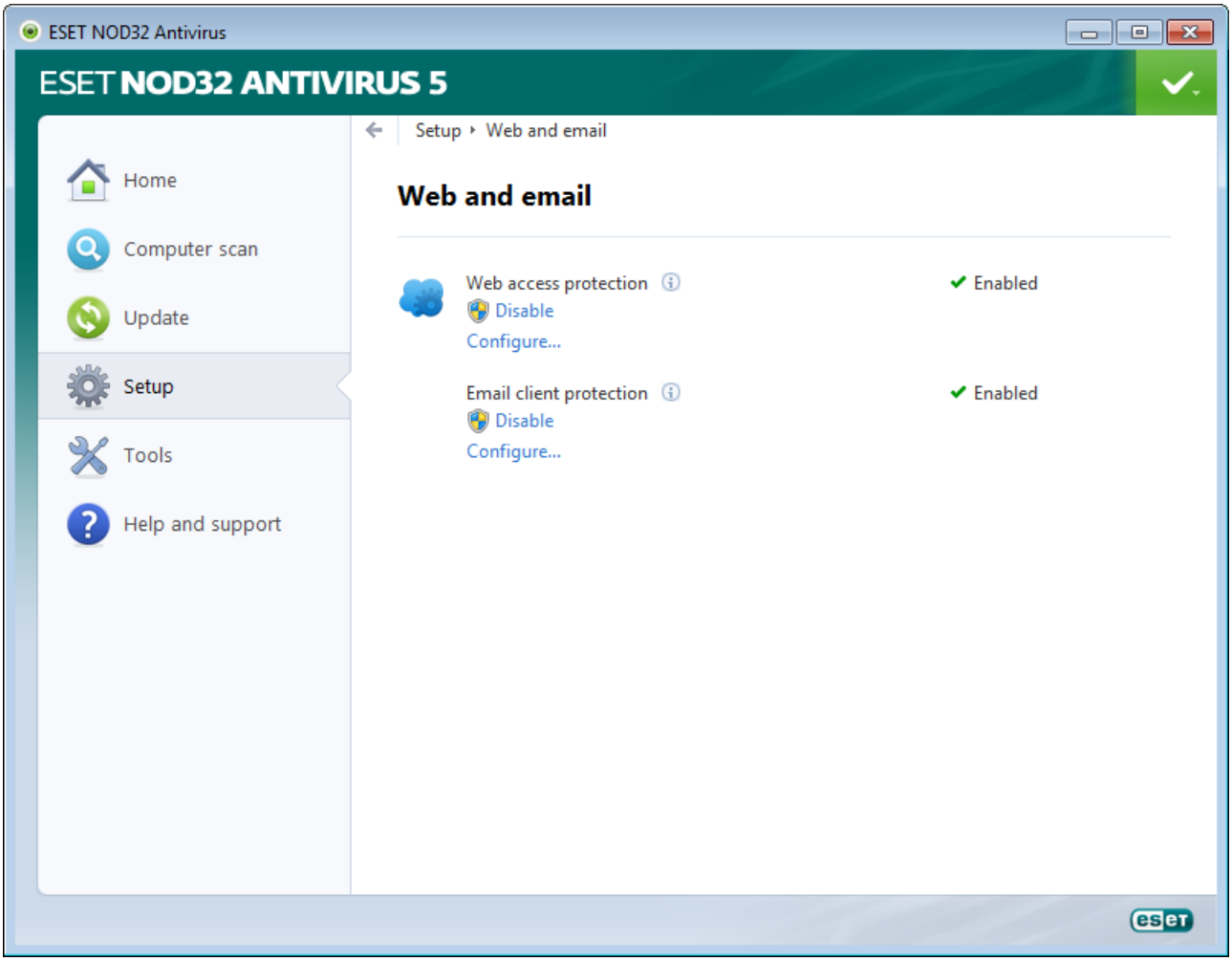

ESET NOD32 Antivirus 5
Allow access to another application?
HIPS
Application: C:\Windows\System32\svchost.exe
Access type: Modify state of another application
Target: C:\Program Files\Windows Live\Companion \companionuser.exe
Allow
Application will be allowed to continue this operation or to perform this action.
Deny
Application won't be allowed to continue this operation or to perform this action.
Create rule
Temporarily remember this action for this process
Hide advanced options
Create a rule valid only for this process
Create a rule valid only for operation
All operations mentioned above
Create a rule valid only for target
C:\Program Files\Windows Live\Companion\companionuser.exe

The dialog window allows rule creation, based on the action that triggered it and the conditions for this action. The exact parameters can be set after clicking on **Show Options**. Rules created like this are considered equal to the rules created manually, so the rule created from a dialog window can be less specific than the rule that triggered the dialog window. This means, that after creating such a rule, the same operation can trigger the same window.

The **Temporarily remember this action for this process** option causes the action (**Allow** / **Deny**) to be remembered for this process and will be used every time this operation triggers a dialog window. These settings are only temporary. After a change of rules or filtering mode, a HIPS module update or a system restart, they will be deleted.

4.2 Web and email

Web and email configuration can be found in the **Setup** pane after clicking on the **Web and email** title. From here you can also access more detailed settings of the program.



Internet connectivity is a standard feature for personal computers. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your **Web access protection**.

Email client protection provides control of email communication received through the POP3 and IMAP protocol. Using the plug-in program for your email client, ESET NOD32 Antivirus provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP).

Disable – Deactivates web/email protection for email clients.

Configure ... – Opens web/email protection advanced settings.

4.2.1 Web access protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection.

We strongly recommend that the Web access protection option is enabled. This option is located in **Setup** > **Web and email** > **Web access protection**.

4.2.1.1 HTTP, HTTPs

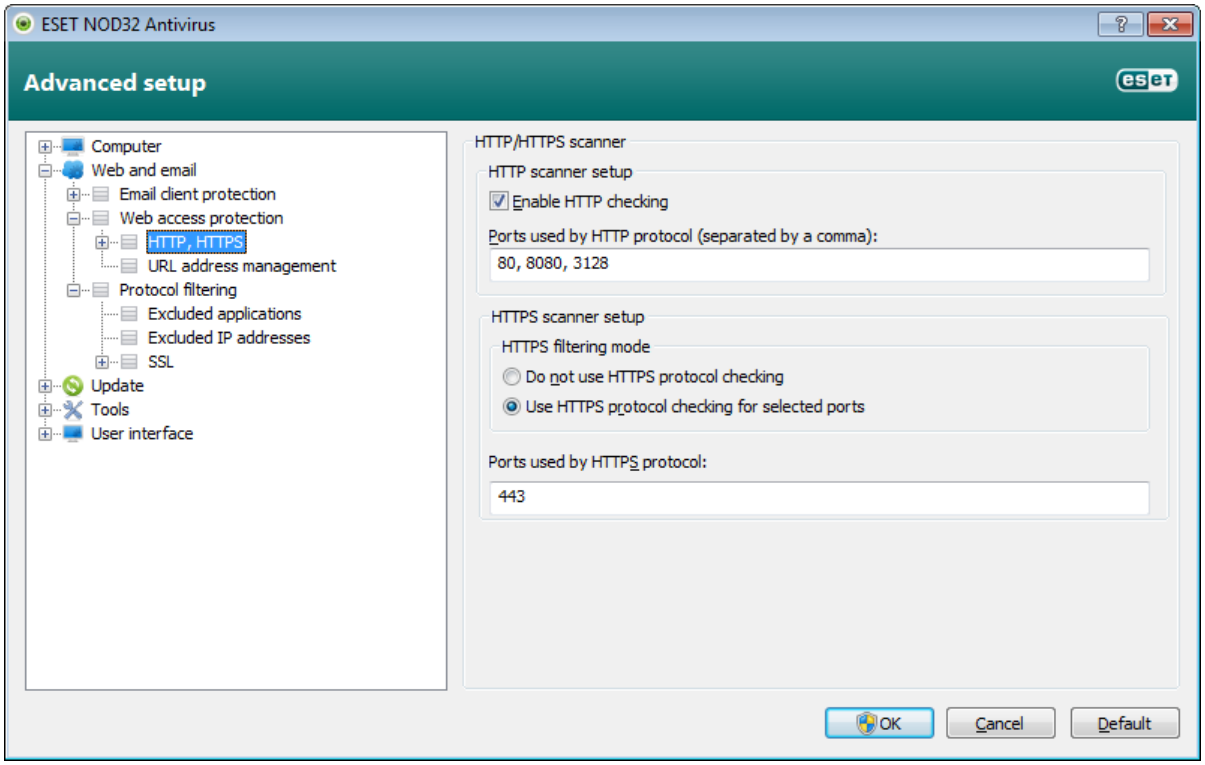
Web access protection works by monitoring communication between web browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPs (encrypted communication) rules. ESET NOD32 Antivirus supports HTTPS protocol checking. This type of communication uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communications utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) encryption methods. By default, ESET NOD32 Antivirus is configured to use the standards of most Internet browsers. However, the HTTP scanner setup options can be modified in **Advanced Setup** (F5) > **Antivirus and antispyware** > **Web access protection** > **HTTP, HTTPs**. In the main HTTP filter window, you can select or deselect the **Enable HTTP checking** option. You can also define the port numbers used for HTTP communication. By default, the port numbers 80, 8080 and 3128 are predefined. HTTPs checking can be performed in the following modes:

Do not use HTTPs protocol checking – Encrypted communication will not be checked.

Use HTTPs protocol checking for selected ports – HTTPs checking only for ports defined in **Ports used by HTTPs protocol**.

Use HTTPS protocol checking for selected ports – The program will only check those applications that are specified in the browsers section and that use ports defined in **Ports used by HTTPS protocol**. Port 443 is set by default.

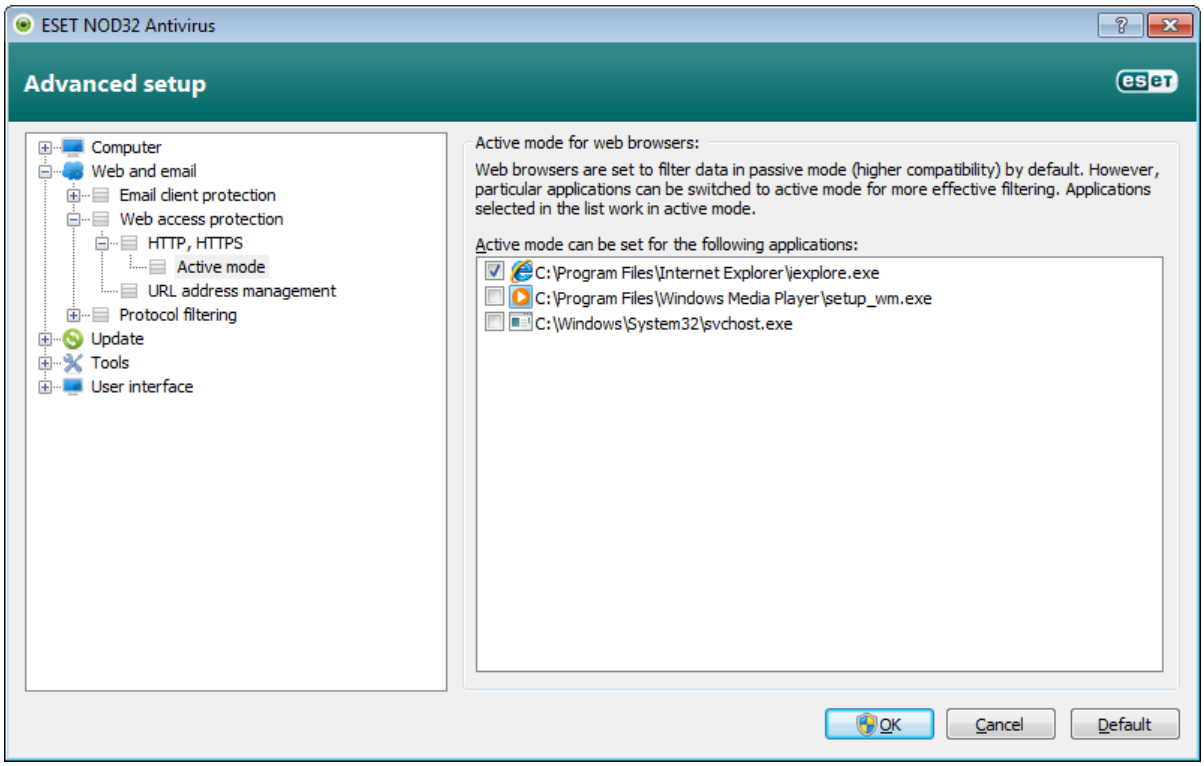
Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL protocol checking in Advanced setup section (**Web and email** > **Protocol filtering** > **SSL**) and enable the **Always scan SSL protocol** option.



4.2.1.1.1 Active mode for web browsers

ESET NOD32 Antivirus also contains the **Active mode** submenu, which defines the checking mode for web browsers.

Active mode is useful because it examines transferred data from applications accessing the Internet as a whole, regardless of whether they are marked as web browsers or not (for more information, see Web and email clients). If it is not enabled, communication from applications are monitored gradually in batches. This decreases the effectiveness of the data verification process, but also provides higher compatibility for listed applications. If no problems occur while using it, we recommend that you enable active checking mode by selecting the checkbox next to the desired application.This is how the active mode works: When a controlled application downloads data, it is first saved to a temporary file created by ESET NOD32 Antivirus. Data is not available for the given application at that time. Once downloading is complete, it is checked for malicious code. If no infiltration is found, data is sent to the original application. This process provides complete control of the communications made by a controlled application. If passive mode is activated, data is trickle-fed to the original application to avoid timeouts.

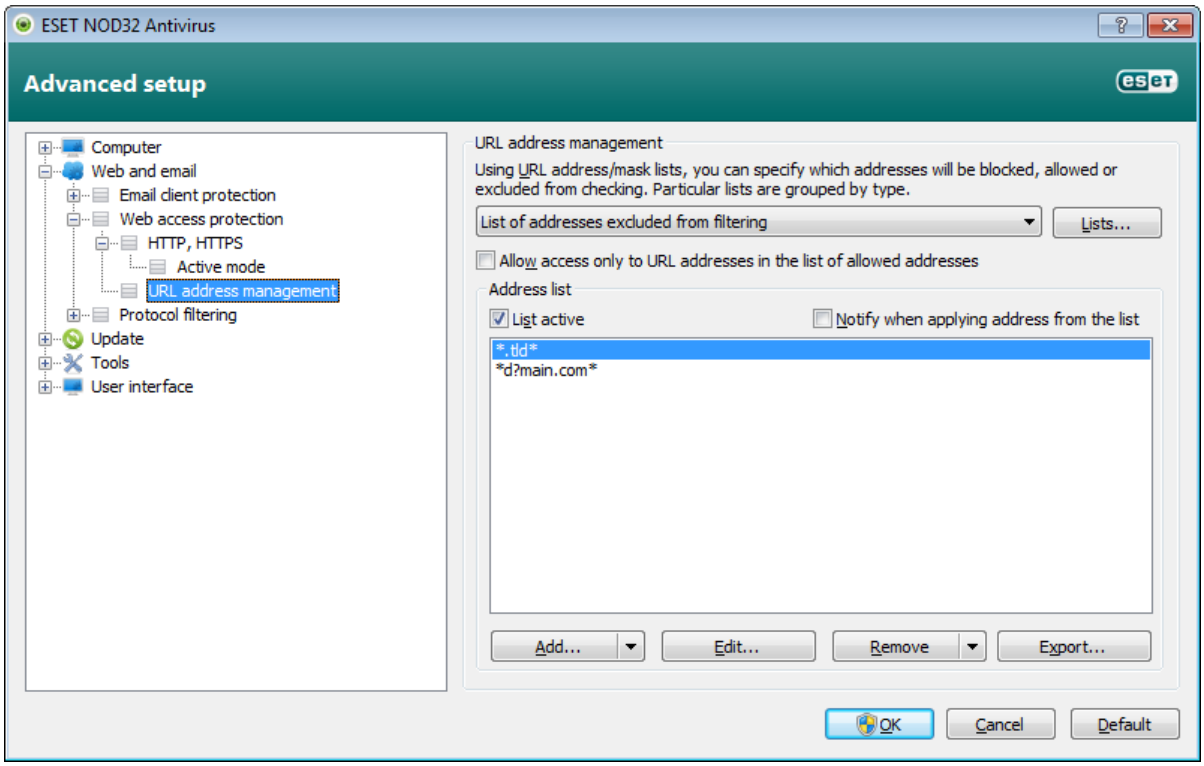


4.2.1.2 URL address management

The URL address management section enables you to specify HTTP addresses to block, allow or exclude from checking. The buttons **Add**, **Edit**, **Remove** and **Export** are used to manage the lists of addresses. Websites in the list of blocked addresses will not be accessible. Websites in the list of excluded addresses are accessed without being scanned for malicious code. If you select the **Allow access only to HTTP addresses in the list of allowed addresses** option, only addresses present in the list of allowed addresses will be accessible, while all other HTTP addresses will be blocked.

If you add a URL address to the **List of addresses excluded from filtering**, the address will be excluded from scanning. You can also allow or block certain addresses, by adding them to the **List of allowed addresses** or **List of blocked addresses**. After you click on the **Lists...** button, a **HTTP address/mask lists** window will pop-up where you can **Add** or **Remove** lists of addresses. In order to add an HTTPS URL addresses to the list, the option **Always scan** SSL protocol has to be active.

In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. To activate a list, select the **List active** option. If you wish to be notified when entering an address from the current list, select **Notify when applying address from the list** option.



Add.../From file – Allows you to add an address to the list, either manually (**Add**), or from a simple text file (**From file**). The **From file** option enables you to add multiple email addresses which are saved in a text file.

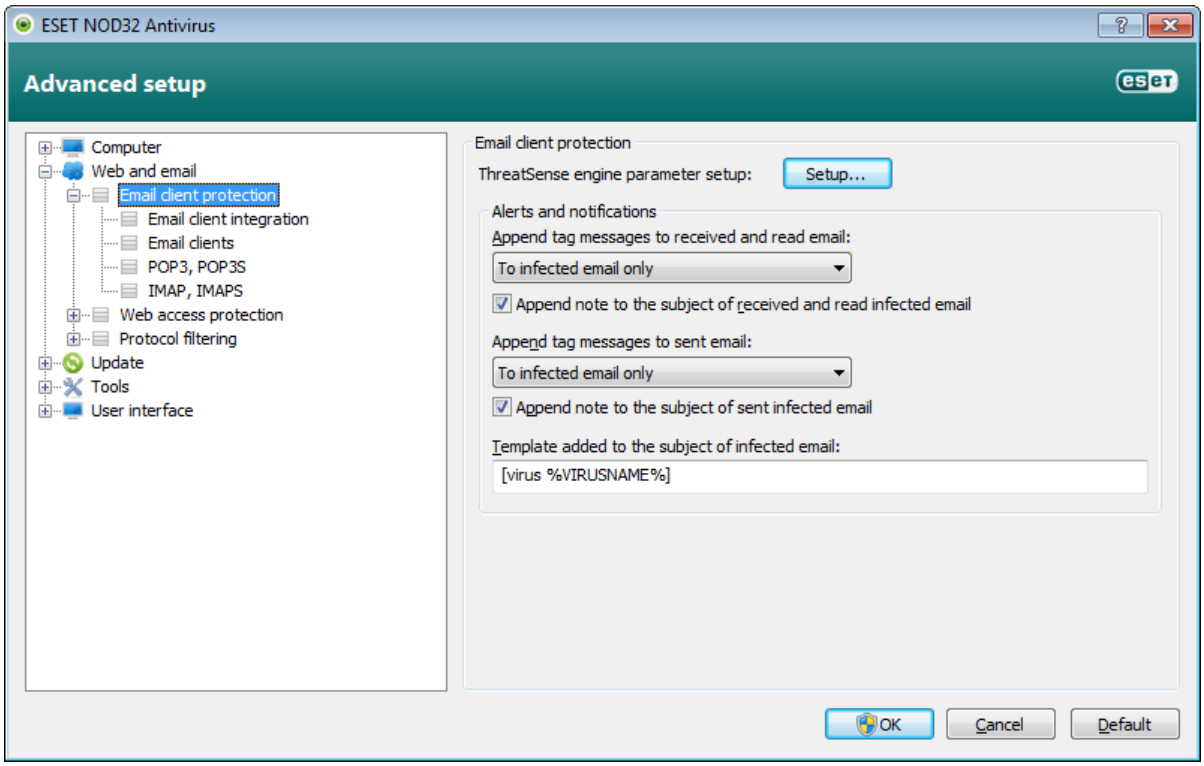
Edit... – Enables you to manually edit addresses – e.g. by adding a mask ("*" and "?").

Remove/Remove all – Click **Remove** to delete the selected address from the list. To delete all addresses, select **Remove all**.

Export... – This option enables you to save addresses from the current list to a simple text file.

4.2.2 Email client protection

Email protection provides control of email communication received through the POP3 and IMAP protocols. Using the plug-in for Microsoft Outlook and other e-mail clients, ESET NOD32 Antivirus provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all the advanced scanning methods provided by the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 and IMAP protocol communications is independent of the email client used.



The options for this functionality are available through **Advanced setup** > **Web and email** > **Email client protection**.

ThreatSense engine parameter setup – The advanced virus scanner setup enables you to configure scan targets, detection methods, etc. Click **Setup...** to display the detailed virus scanner setup window.

After an email has been checked, a notification with the scan result can be appended to the message. You can select to **Append tag messages to received and read mail**, as well as **Append tag messages to sent mail**. The tag messages cannot be relied on without question, since they may be omitted in problematic HTML messages or can be forged by some viruses. The tag messages can be added either to received and read email or to sent email (or both). The available options are:

- **Never** – No tag messages will be added at all.
- **To infected email only** – Only messages containing malicious software will be marked as checked (default).
- **To all scanned email** – The program will append messages to all scanned email.

Append note to the subject of received and read/sent infected email – Enable this checkbox if you want email protection to include a virus warning in the subject of an infected email. This feature allows for simple, subject-based filtering of infected emails (if supported by your email program). It also increases the level of credibility for the recipient and, if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

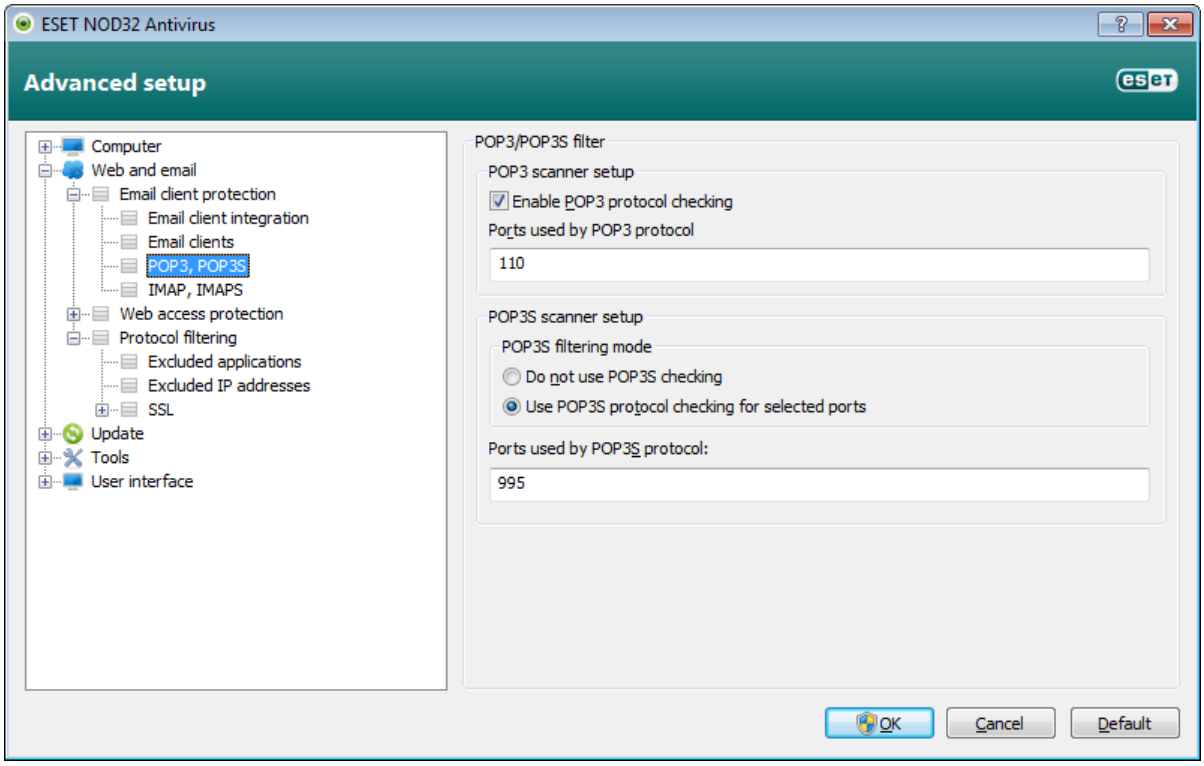
Template added to the subject of infected email – Edit this template if you wish to modify the subject prefix format of an infected email. This function will replace the message subject *"Hello"* with a given prefix value *"[virus]"* to the following format: *"[virus] Hello"*. The variable *%VIRUSNAME%* represents the detected threat.

4.2.2.1 POP3, POP3S filter

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET NOD32 Antivirus provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 protocol checking is performed automatically with no need for reconfigure the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL protocol checking in Advanced setup section (**Web and email** > **Protocol filtering** > **SSL**) and enable the **Always scan SSL protocol** option.



In this section, you can configure POP3 and POP3S protocol checking.

Enable POP3 protocol checking – If enabled, all traffic through POP3 is monitored for malicious software.

Ports used by POP3 protocol – A list of ports used by the POP3 protocol (110 by default).

ESET NOD32 Antivirus supports also POP3S protocol checking. This type of communication uses an encrypted channel to transfer information between server and client. ESET NOD32 Antivirus checks communications utilizing the SSL (Secure Socket Layer), and TLS (Transport Layer Security) encryption methods.

Do not use POP3S checking – Encrypted communication will not be checked.

Use POP3S protocol checking for selected ports – Check this option to enable POP3S checking only for ports defined in **Ports used by POP3S protocol**.

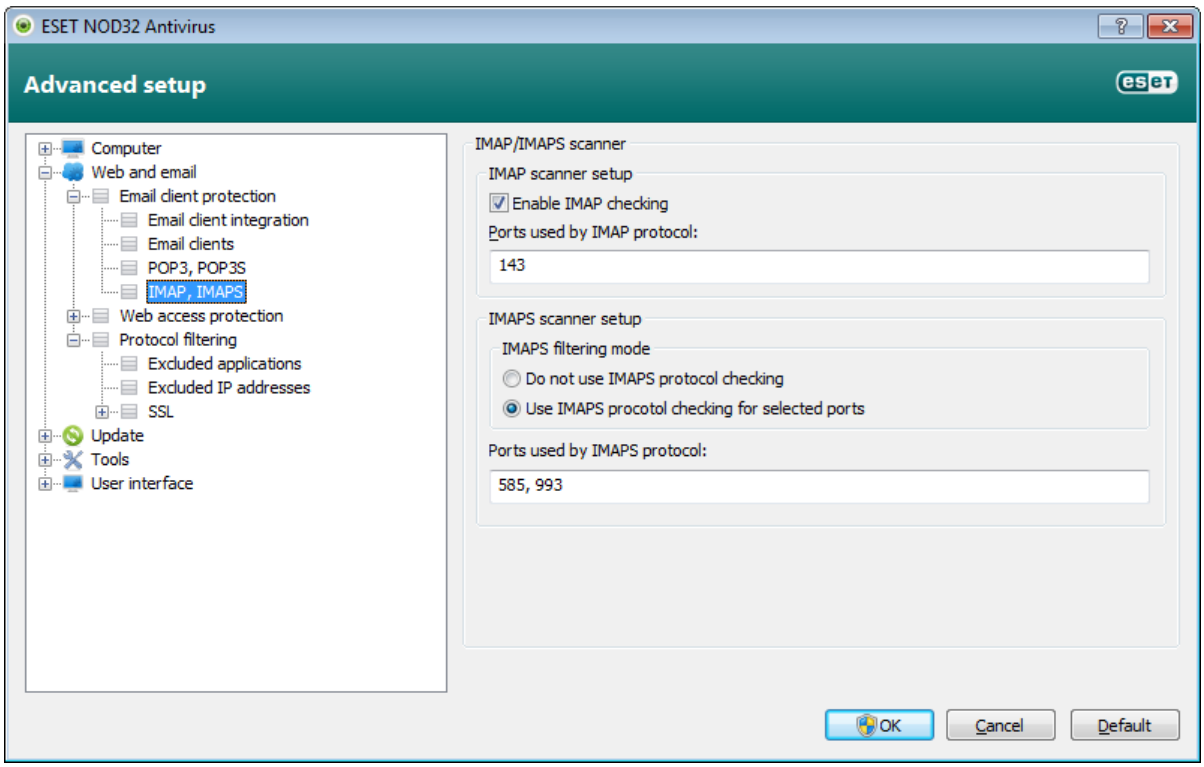
Ports used by POP3S protocol – A list of POP3S ports to check (995 by default).

4.2.2.2 IMAP, IMAPS protocol control

The Internet Message Access Protocol (IMAP) is another Internet protocol for e-mail retrieval. IMAP has some advantages over POP3, e.g., multiple clients can simultaneously connect to the same mailbox and maintain message state information such as whether or not the message has been read, replied to or deleted. ESET NOD32 Antivirus provides protection for this protocol, regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled; IMAP protocol control is performed automatically with no need for reconfigure the email client. By default, all communication on port 143 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

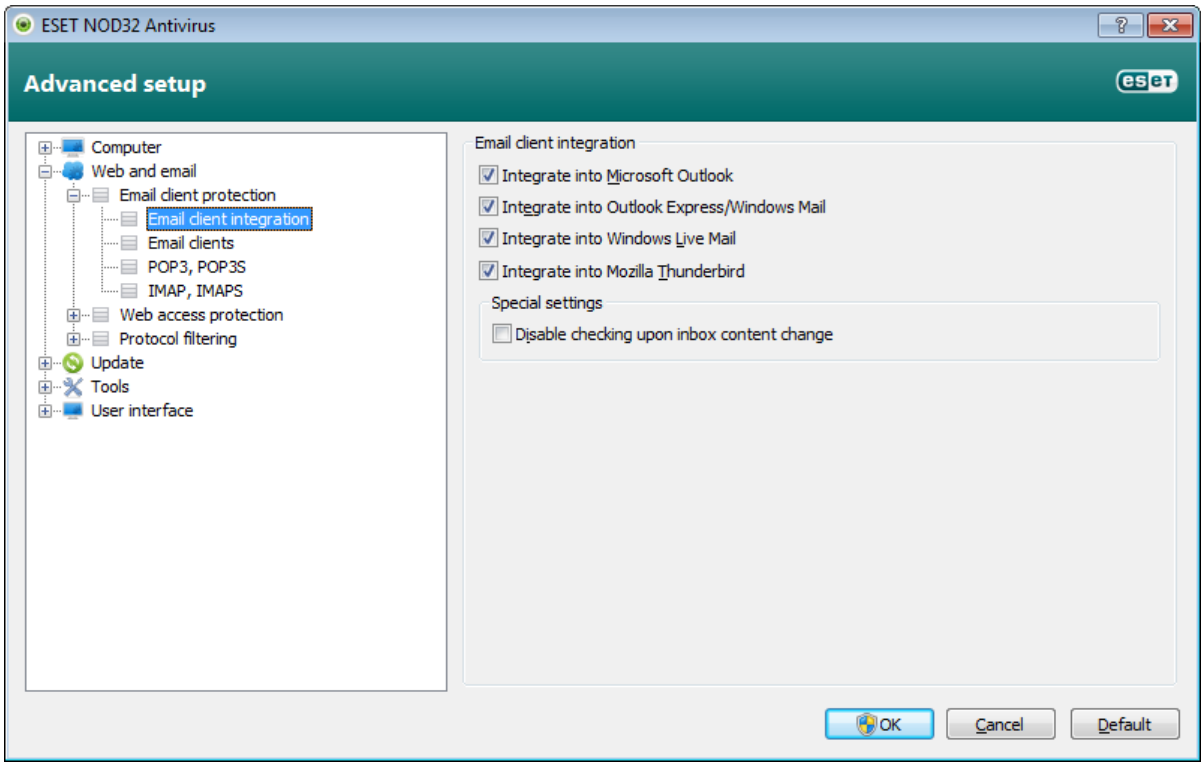
Encrypted communication will be not scanned. To enable the scanning of encrypted communication and view the scanner setup, navigate to SSL protocol checking in Advanced setup section (**Web and email** > **Protocol filtering** > **SSL**) and enable the **Always scan SSL protocol** option.



4.2.2.3 Integration with email clients

Integration of ESET NOD32 Antivirus with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, this integration can be enabled in ESET NOD32 Antivirus. If integration is activated, the ESET NOD32 Antivirus toolbar is inserted directly into the email client, allowing for more efficient email protection. The integration settings are available through **Setup** > **Enter advanced setup...** > **Web and email** > **Email client protection > Email client integration**. Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird.

Select the **Disable checking upon inbox content change** option if you are experiencing a system slowdown when working with your email client. Such a situation may take place when downloading email from Kerio Outlook Connector Store.



4.2.2.3.1 Email client protection configuration

The Email protection module supports the following email clients: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird. Email protection works as a plug-in for these programs. The main advantage of the plug-in control is that it is independent of the protocol used. When the email client receives an encrypted message, it is decrypted and sent to the virus scanner.

Email to scan

Received email – Toggles checking of received messages.
Sent email – Toggles checking of sent messages.
Read email – Toggles checking of read messages.

Action to be performed on infected email

No action – If enabled, the program will identify infected attachments, but will leave emails without taking any action.
Delete email – The program will notify the user about infiltration(s) and delete the message.
Move email to the Deleted items folder – Infected emails will be moved automatically to the **Deleted items** folder.
Move email to folder – Specify the custom folder you wish to move the infected email to when detected.

Other

Repeat scan after update – Toggles rescanning after a virus signature database update.
Accept scan results from other modules – If this option is selected, the email protection module accepts scan results of other protection modules.

4.2.2.4 Removing infiltrations

If an infected email message is received, an alert window will display. The alert window shows the sender name, email and the name of the infiltration. In the lower part of the window the options **Clean**, **Delete** or **Leave** are available for the detected object. In almost all cases, we recommend that you select either **Clean** or **Delete**. In certain situations, if you wish to receive the infected file, select **Leave**. If **Strict cleaning** is enabled, an information window with no options available for infected objects will displayed.

4.2.3 Protocol filtering

Antivirus protection for the application protocols is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. The control works automatically, regardless of the Internet browser or email client used. For encrypted (SSL) communication see **Protocol filtering** > **SSL**.

Integrate into system – Enables the driver for the ESET NOD32 Antivirus protocol filtering functionality.

Enable application protocol content filtering – If enabled, all HTTP(S), POP3(S) and IMAP(S) traffic will be checked by the antivirus scanner.

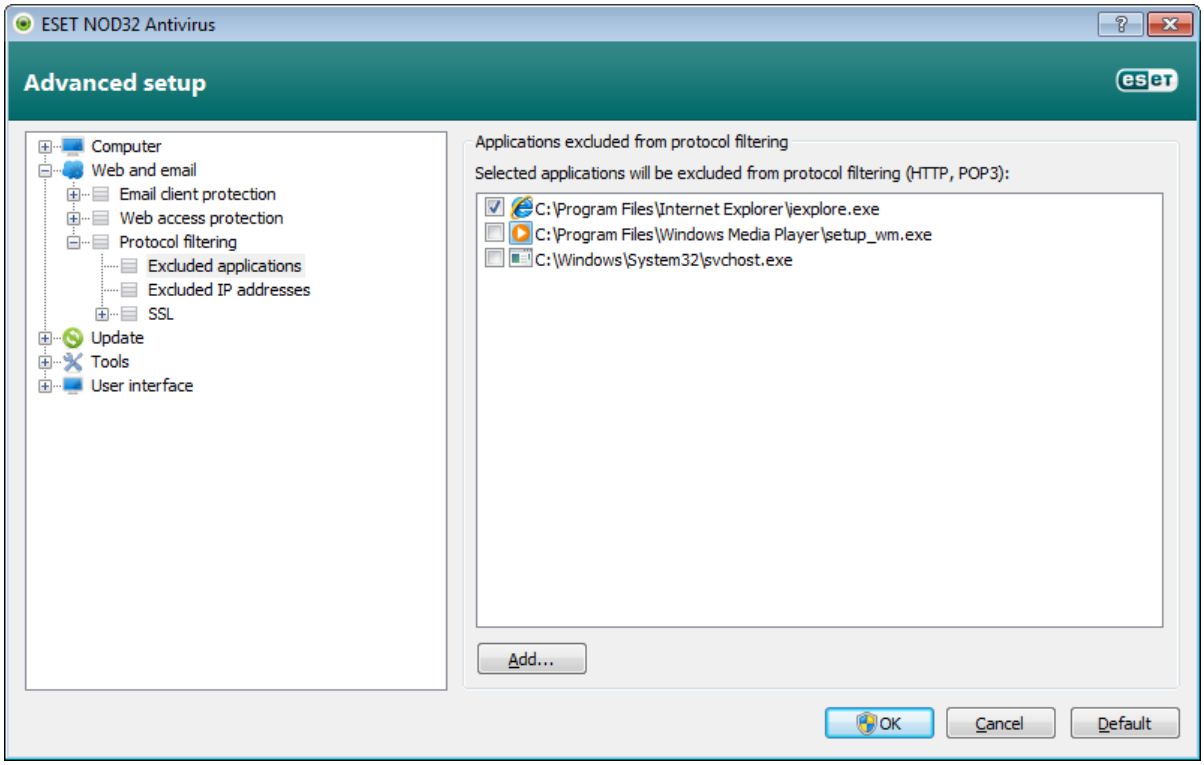
NOTE: Starting with Windows Vista Service Pack 1, Windows 7 and Windows Server 2008, the new Windows Filtering Platform (WFP) architecture is used to check network communication. Since the WFP technology uses special monitoring techniques, the following options are not available.

- **HTTP and POP3 ports** – Limits routing the traffic to the internal proxy server only for HTTP and POP3 ports.
- **Applications marked as web browsers and email clients** – Limits routing the traffic to the internal proxy server only for the applications marked as browsers and email clients (**Web and email** > **Protocol filtering** > **Web and email clients**).
- **Ports and applications marked as web browsers or email clients** – Enables routing of all traffic on HTTP and POP3 ports as well as all the communication of the applications marked as browsers and email clients on the internal proxy server.

4.2.3.1 Excluded applications

To exclude communication of specific network-aware applications from content filtering, select them in the list. HTTP/POP3/IMAP communication of the selected applications will not be checked for threats. We recommend using this option only for applications that do not work properly with their communication being checked.

Running applications and services will be available here automatically. Click the **Add...** button to manually select an application not shown on the protocol filtering list.

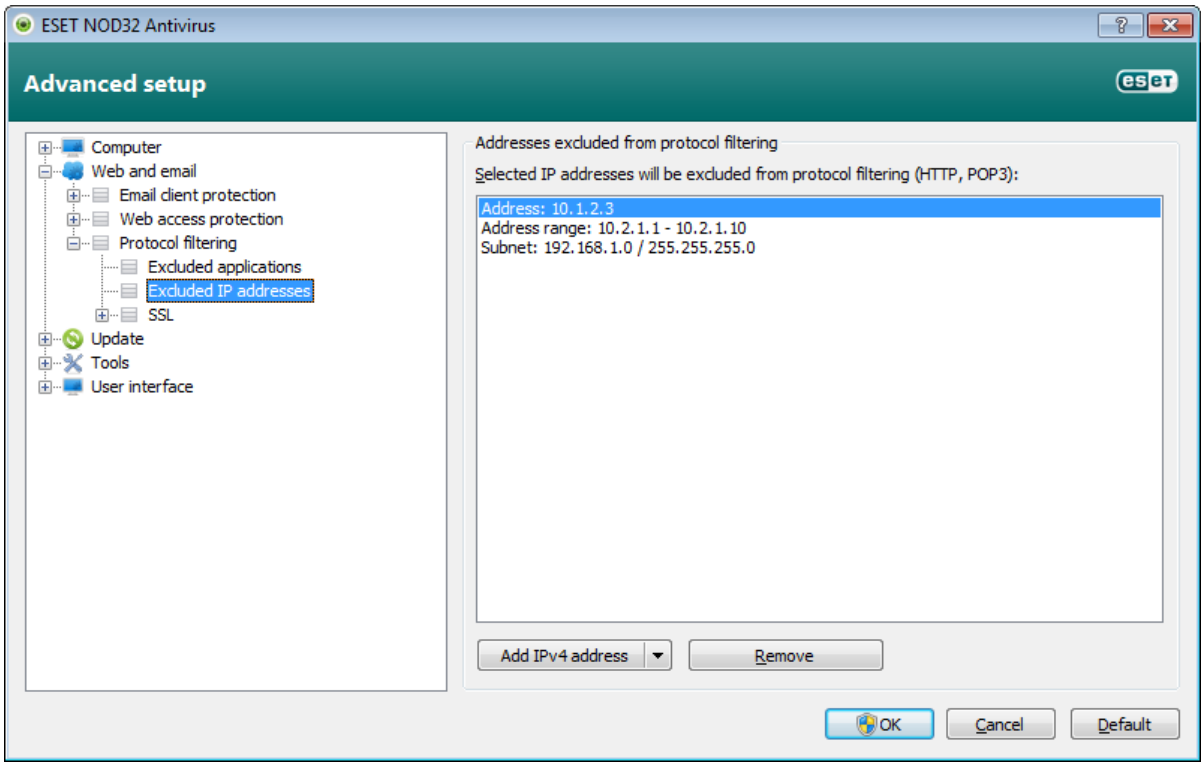


4.2.3.2 Excluded addresses

The entries in the addresses list will be excluded from the content filtering. HTTP/POP3 communication from/to the selected addresses will not be checked for threats. We recommend using this option only for addresses that are trustworthy.

Add IPv4 address – This options allows you to add an IP address/address range/subnet of a remote point for which the rule is to be applied.

Remove – Remove selected entries from the list.



4.2.3.3 SSL protocol checking

ESET NOD32 Antivirus enables you to check protocols encapsulated in SSL protocol. You can use various scanning modes for SSL protected communications using trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Always scan SSL protocol – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked by you as trusted (it is added to the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

Ask about non-visited sites (exclusions can be set) – If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode enables you to create a list of SSL certificates that will be excluded from scanning.

Do not scan SSL protocol – If selected, the program will not scan communications over SSL.

Apply created exceptions based on certificates – Activates using exclusions specified in excluded and trusted certificates for scanning SSL communication. This option is available if you select **Always scan SSL protocol**.

Block encrypted communication utilizing the obsolete protocol SSL v2 – Communication using the earlier version of the SSL protocol will be automatically blocked.

4.2.3.3.1 Certificates

For SSL communication to work properly in your browsers/email clients, it is essential that the root certificate for ESET, spol. s r.o. be added in the list of known root certificates (publishers). Therefore, the **Add the root certificate to known browsers** option should be enabled. Select this option to automatically add the ESET root certificate to the known browsers (e.g. Opera, Firefox). For browsers using the system certification store, the certificate is added automatically (e.g. Internet Explorer). To apply the certificate to unsupported browsers, click **View Certificate** > **Details** > **Copy to File...** and then manually import it into the browser.

In some cases, the certificate cannot be verified using the Trusted Root Certification Authorities store (e.g. VeriSign). This means that the certificate is self-signed by someone (e.g. administrator of a web server or a small business company) and considering this certificate as trusted is not always a risk. Most large business companies (e.g. banks) use certificate signed by TRCA. If the **Ask about certificate validity** option (default) is set, the user will be prompted to select an action to take when encrypted communication is established. An action selection dialog will be displayed, where you can decide to mark the certificate as trusted or excluded. If the certificate is not present in the TRCA list, the window is red. If the certificate is on the TRCA list, the window will be green.

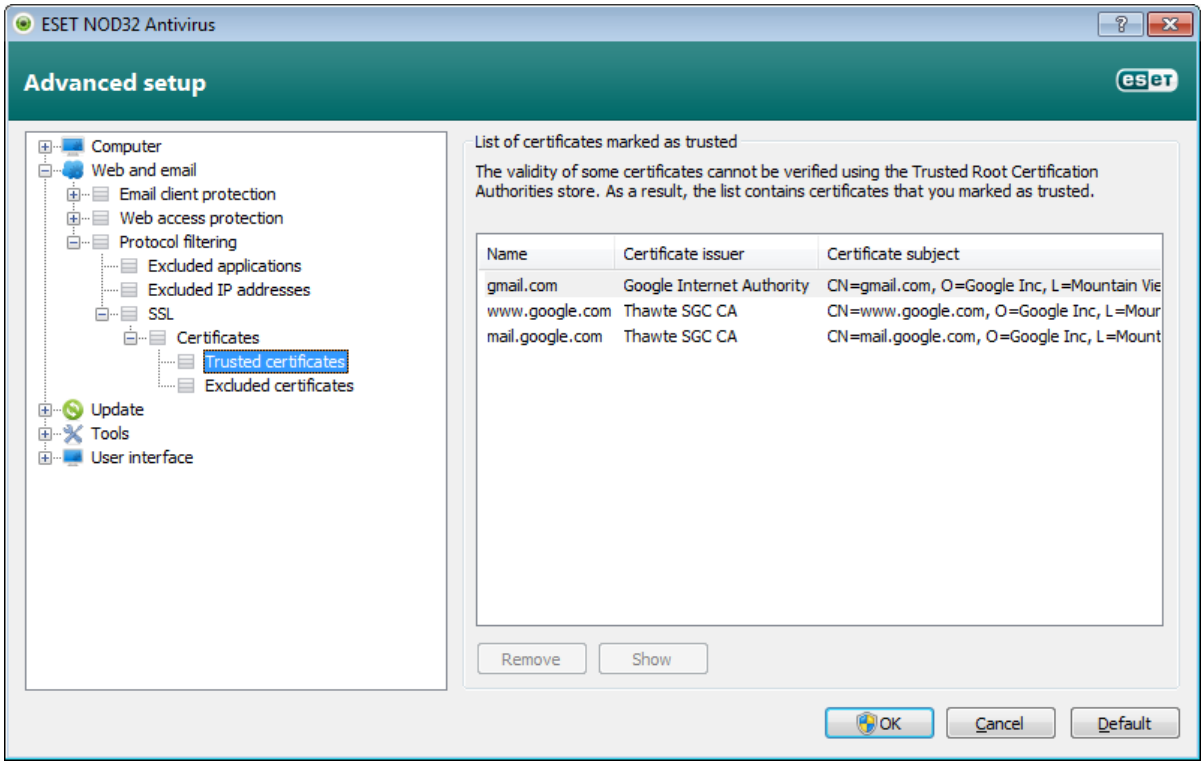
ESET NOD32 Antivirus 5
Encrypted SSL communication
Untrusted certificate
An application running on this computer is attempting to communicate over encrypted SSL channel. If you want to check the encrypted channel content, mark the certificate as trusted.
Do you consider the remote computer's certificate trusted?
Application:
Internet Explorer
Certificate:
www.sk-nic.sk
Yes
Yes, always
No
Exclude

You can set the **Block communication that uses the certificate** option to always terminate an encrypted connection to the site that uses the unverified certificate.

If the certificate is invalid or corrupt, it means that the certificate expired or was incorrectly self-signed. In this case, we recommend that you block the communication that uses the certificate.

4.2.3.3.1.1 Trusted certificates

In addition to the integrated Trusted Root Certification Authorities store where ESET NOD32 Antivirus stores trusted certificates, you can create a custom list of trusted certificates that can be viewed in **Advanced Setup** (F5) > **Web and email** > **Protocol filtering** > **SSL** > **Certificates** > **Trusted certificates**. ESET NOD32 Antivirus will check the content of encrypted communications utilizing certificates in this list.



To delete the selected items from the list, click the **Remove** button. Click the **Show** option (or double-click the certificate) to display information about the selected certificate.

4.2.3.3.1.2 Excluded certificates

The Excluded certificates section contains certificates that are considered safe. The content of encrypted communications utilizing the certificates in the list will not be checked for threats. We recommend only excluding web certificates that are guaranteed to be safe and the communication utilizing the certificates does not need to be checked. To delete selected items from the list, click the **Remove** button. Click the **Show** option (or double-click the certificate) to display information about the selected certificate.

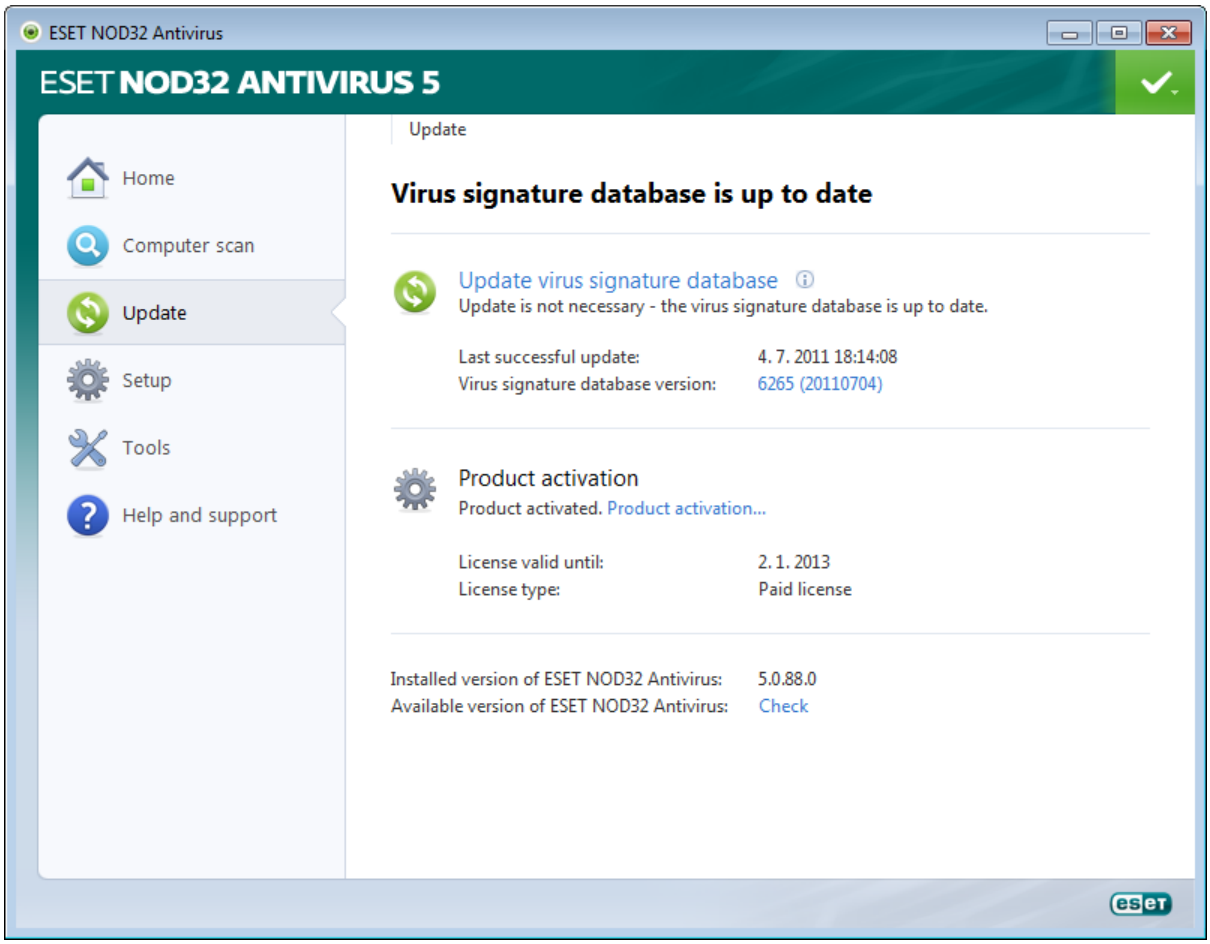
4.3 Updating the program

Regularly updating ESET NOD32 Antivirus is the best method to obtain the maximum level of security on your computer. The Update module ensures that the program is always up to date in two ways – by updating the virus signature database and by updating system components.

By clicking **Update** from the main menu, you can find the current update status, including the date and time of the last successful update and if an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added within the given update.

In addition, the option to manually begin the update process – **Update virus signature database** – is available. Updating the virus signature database and updating program components are an important part of providing complete protection against malicious code. Please pay attention to their configuration and operation. If you did not enter the License details during installation, you can enter your username and password when updating to access ESET's update servers.

NOTE: The username and password are provided by ESET after purchasing ESET NOD32 Antivirus.



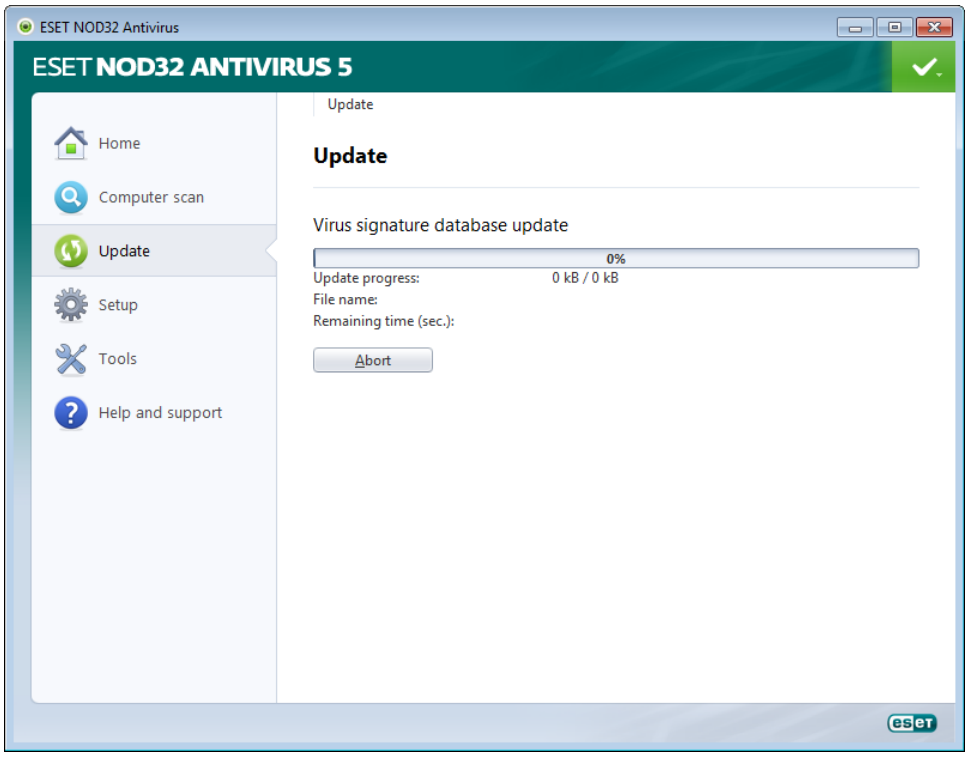
Last successful update – The date of the last update. Make sure it refers to a recent date, which means that the virus signature database is current.

Virus signature database version – The virus signature database number, which is also an active link to ESET's website. Click it to view listing all signatures added within the given update.

Click **Check** to detect the latest **Available version of ESET NOD32 Antivirus** of your ESET security product.

Update process

After clicking **Update virus signature database**, the download process begins. A download progress bar and remaining time to download will be displayed. To interrupt the update, click **Abort**.

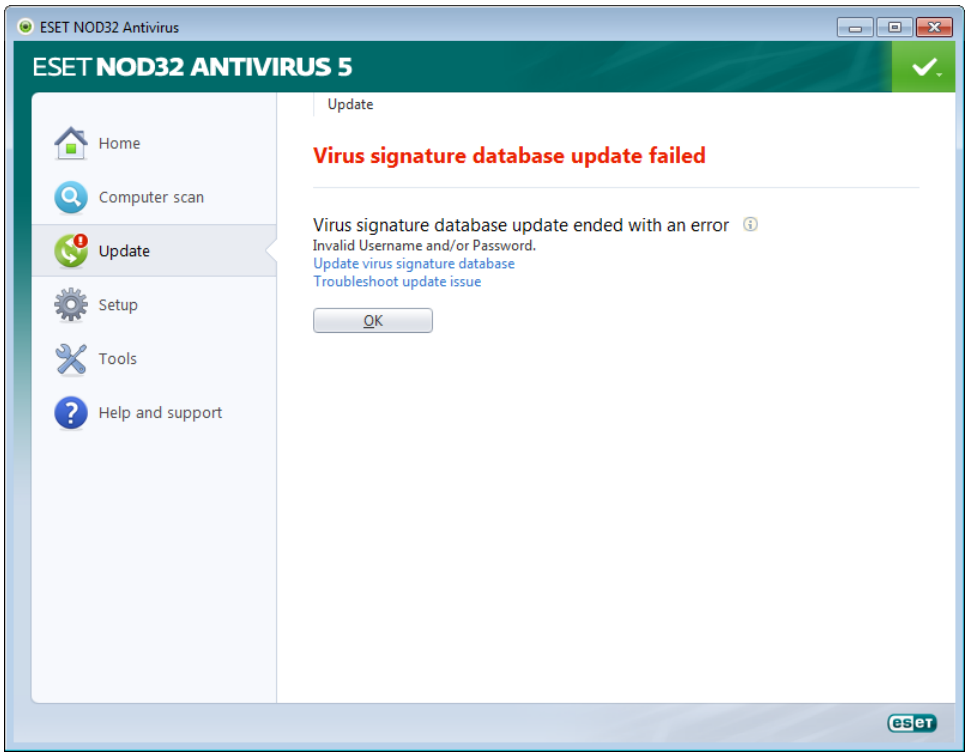


Important: Under normal circumstances, when updates are downloaded properly, the message **Update is not necessary – Virus signature database is up to date** will appear in the **Update** window. If this is not the case, the program is out of date, which increases the risk of infection. Please update the virus signature database as soon as possible. Otherwise, one of the following messages will be displayed:

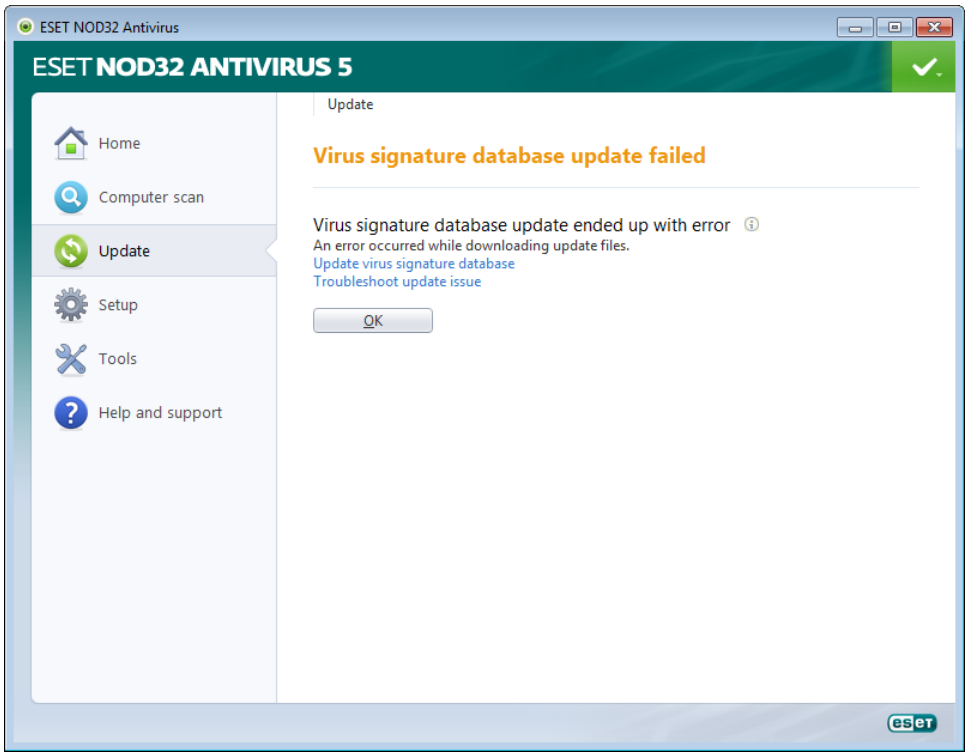
Virus signature database is out of date – This error will appear after several unsuccessful attempts to update the virus signature database. We recommend that you check the update settings. The most common reason for this error is incorrectly entered authentication data or incorrectly configured connection settings.

The previous notification is related to the following two messages about unsuccessful updates:

The username and password have been incorrectly entered in update setup. We recommend that you check your authentication data. The Advanced Setup window (click **Setup** from the main menu and then click **Enter advanced setup...**, or press F5 on your keyboard) contains additional update options. Click **Update** > **Update** from the Advanced Setup tree.



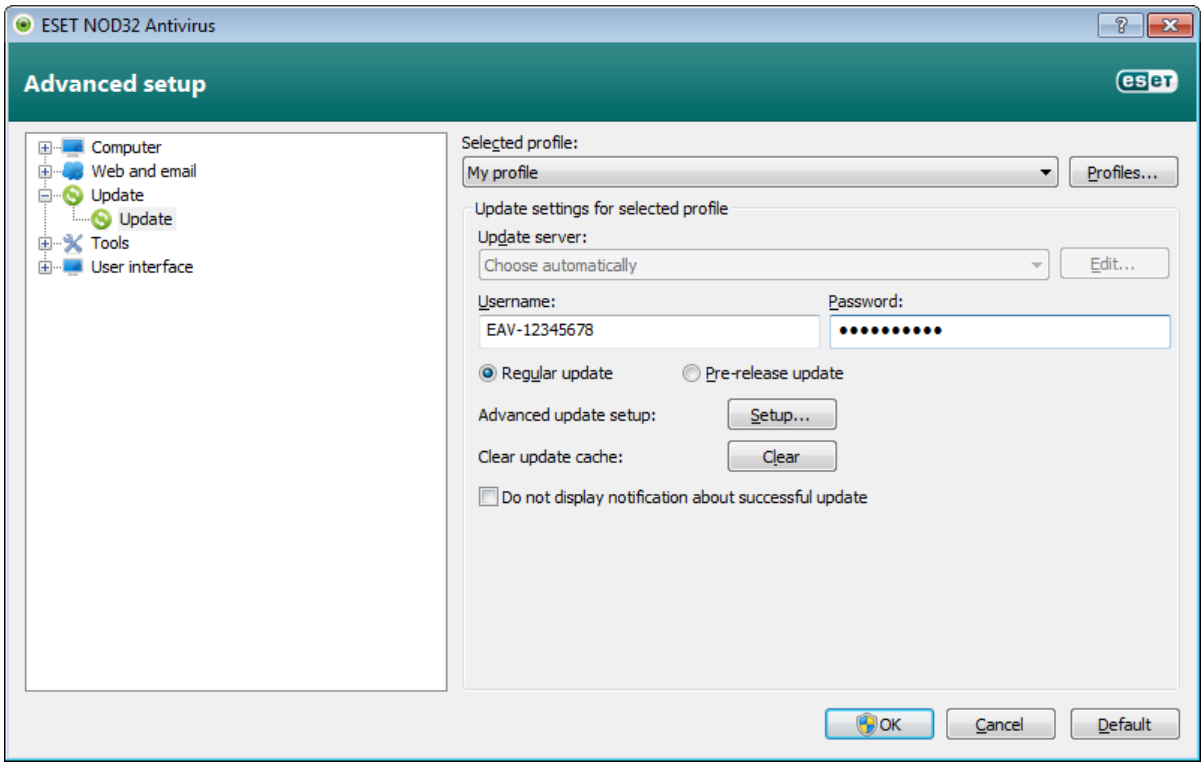
Virus signature database update failed – A possible cause of the error is incorrect Internet connection settings. We recommend that you check your Internet connectivity (by opening any website in your web browser). If the website does not open, it is likely that an Internet connection is not established or there are connectivity problems with your computer. Please check with your Internet Service Provider (ISP) if you do not have an active Internet connection.



4.3.1 Update setup

The update setup section specifies update source information, such as the update servers and authentication data for these servers. By default, the **Update server** drop-down menu is set to **Choose automatically** to ensure that update files will automatically download from the ESET server with the least network traffic. The update setup options are available from the **Advanced Setup** tree (F5 key), under **Update** > **Update**.

For updates to be downloaded properly, it is essential to correctly fill in all parameters. If you use a firewall, please make sure that the program is allowed to communicate with the Internet (i.e., HTTP communication).



The currently used update profile displays the **Selected profile** drop-down menu. Click **Profiles...** to create a new profile.

The list of available update servers is accessible via the **Update server** drop-down menu. The Update server is a location where updates are stored. If you use an ESET server, please leave the default option **Choose automatically** selected. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button. When using a local HTTP server – also known as a Mirror – the update server should be set as follows: *http://computer_name_or_its_IP_address:2221*.

Authentication for update servers is based on the **Username** and **Password** generated and sent to you after purchase. When using a local Mirror server, the verification depends on its configuration. By default, no verification is required, i. e., the **Username** and **Password** fields are left empty.

If the **Pre-release updates** option is enabled, beta-modules will be downloaded during the update, which allows the user to test new features of the product. The list of current modules can be found in **Help and support** > **About ESET NOD32 Antivirus**. It is recommended that basic users leave the **Regular update** option selected by default.

Click the **Setup...** button next to **Advanced update setup** to display a window containing advanced update options.

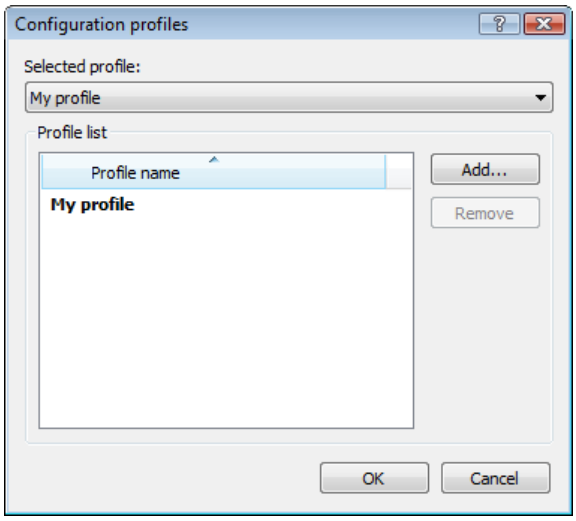
If you experience problems with an update, click the **Clear...** button to flush the folder with temporary update files.

Do not display notification about successful update – Turns off the system tray notification at the bottom right corner of the screen. It is useful to select this option if a full screen application or a game is running. Please note that the Gamer mode will turn off all notifications.

4.3.1.1 Update profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users, who can create an alternative profile for Internet connection properties that regularly change.

The **Selected profile** drop-down menu displays the currently selected profile, set to **My profile** by default. To create a new profile, click the **Profiles...** button and then click the **Add...** button and enter your own **Profile name**. When creating a new profile, you can copy settings from an existing one by selecting it from the **Copy settings from profile** drop-down menu.



In the profile setup window, you can specify the update server from a list of available servers or add a new server. The list of existing update servers is accessible via the **Update server** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

4.3.1.2 Advanced update setup

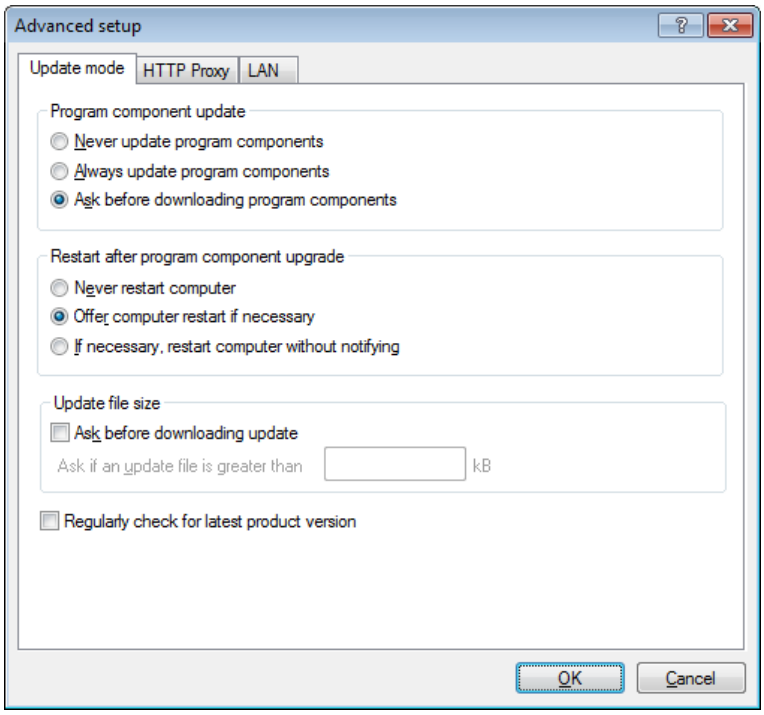
To view the Advanced update setup, click the **Setup...** button. Advanced update setup options include configuration of **Update mode**, **HTTP Proxy** and **LAN**.

4.3.1.2.1 Update mode

The **Update mode** tab contains options related to the program component update. The program enables you to predefine its behavior if a new program component upgrade is available.

The program component upgrade brings new features or makes changes to those that already exist from previous versions. It can be performed automatically without user intervention, or you can choose to be notified. After a program component upgrade has been installed, a computer restart may be required. In the **Program component update** section, three options are available:

- **Never update program components** – Program component updates will not be performed at all. This option is suitable for server installations, since servers can usually be restarted only when they are undergoing maintenance.
- **Always update program components** – A program component upgrade will be downloaded and installed automatically. Please remember that a computer restart may be required.
- **Ask before downloading program components** – The default option. You will be prompted to confirm or refuse program component updates when they are available.



After a program component update, it may be necessary to restart your computer to provide full functionality of all modules. The **Restart after program component upgrade** section allows you to select one of the following options:

- **Never restart computer** – You will not be asked to restart, even if it is required. Please note that this is not recommended, since your computer might not work properly until the next restart.
- **Offer computer restart if necessary** – The default option. After a program component upgrade, you will be prompted to restart your computer in a dialog window.
- **If necessary, restart computer without notifying** – After a program component upgrade, your computer will be restarted (if required).

NOTE: Selecting the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers – e.g., restarting the server automatically after a program upgrade could cause serious damage.

If the **Ask before downloading update** option is checked, a notification will display when a new update is available.

If the update file size is greater than the specified **Ask if an update file is greater than** value, the program will display notification.

The **Regularly check for latest product version** option will enable the **Regular checking for latest product version** scheduled task (see chapter Scheduler).

4.3.1.2.2 Proxy server

To access the proxy server setup options for a given update profile, click **Update** in the Advanced Setup tree (F5) and then click the **Setup...** button to the right of **Advanced update setup**. Click the **HTTP Proxy** tab and select one of the three following options:

- **Use global proxy server settings**
- **Do not use proxy server**
- **Connection through a proxy server**

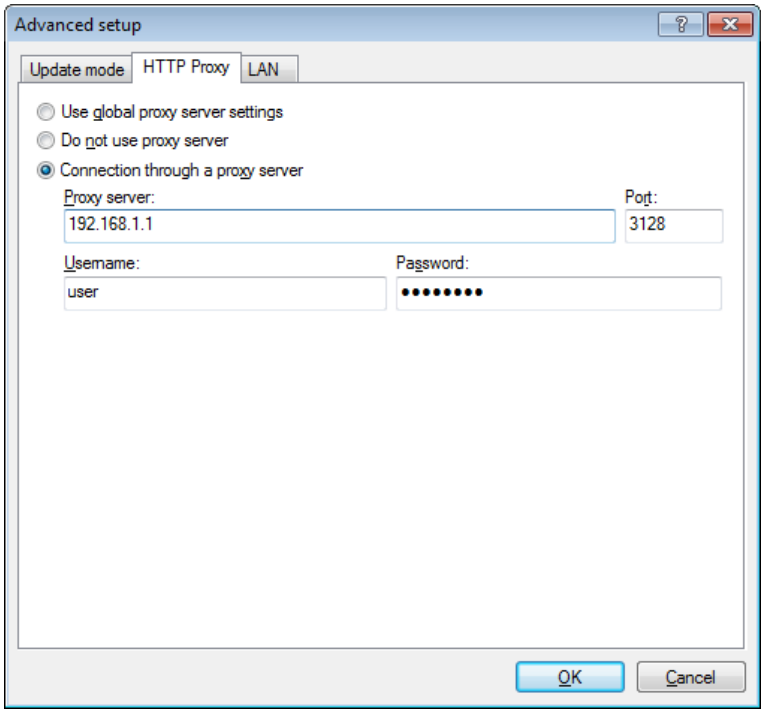
Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Tools** > **Proxy server** branch of the Advanced Setup tree.

Select the **Do not use proxy server** option to specify that no proxy server will be used to update ESET NOD32 Antivirus.

The **Connection through a proxy server** option should be selected if:

- A proxy server should be used to update ESET NOD32 Antivirus and is different from the proxy server specified in the global settings (**Tools** > **Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port**, plus **Username** and **Password** for the proxy server, if required.
- The proxy server settings were not set globally, but ESET NOD32 Antivirus will connect to a proxy server for updates.
- Your computer is connected to the Internet via a proxy server. The settings are taken from Internet Explorer during

program installation, but if they are subsequently changed (e.g. if you change your ISP), please check that the HTTP proxy settings are correct in this window. Otherwise the program will not be able to connect to the update servers.



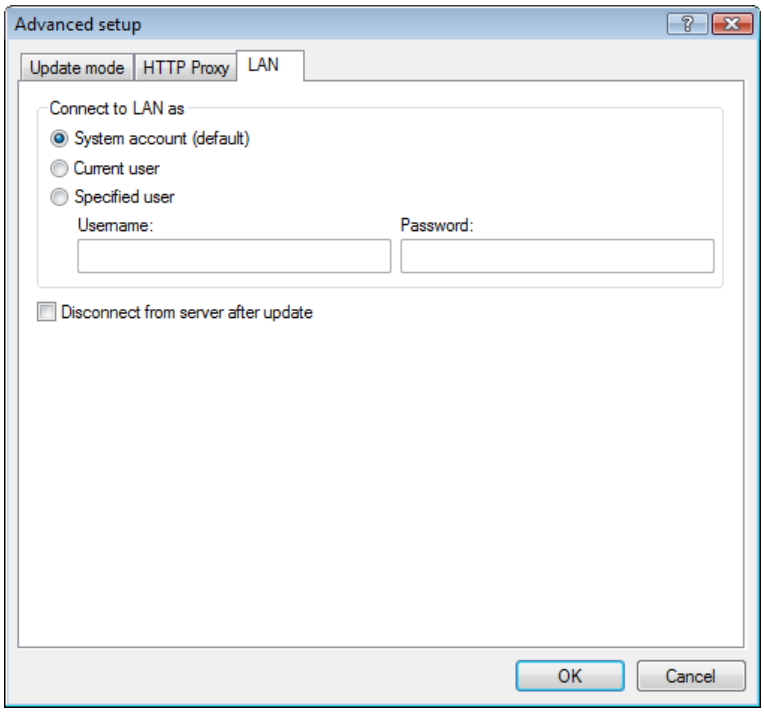
The default setting for the proxy server is **Use global proxy server settings**.

NOTE: Authentication data such as **Username** and **Password** are intended for accessing the proxy server. Fill in these fields only if a username and password are required. Please note that these fields are not for your username/password for ESET NOD32 Antivirus, and should only be supplied if you know you need a password to access the internet via a proxy server.

4.3.1.2.3 Connecting to the LAN

When updating from a local server with an NT-based operating system, authentication for each network connection is required by default. In most cases, a local system account does not have sufficient rights to access the Mirror folder (the Mirror folder contains copies of update files). If this is the case, enter the username and password in the update setup section or specify an existing account under which the program will access the update server (Mirror).

To configure such an account, click the **LAN** tab. The **Connect to LAN as** section offers the **System account (default)**, **Current user**, and **Specified user** options.



Select the **System account (default)** option to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select **Specified user** if you want the program to use a specific user account for authentication. Use this method when the system account connection failed. Please be aware that the specified user account must have access to the update files directory on the local server. Otherwise the program will not be able to establish a connection and download updates.

Warning: When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend inserting the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: *domain_name\user* (if it is a workgroup, enter *workgroup_name\name*) and password. When updating from the HTTP version of the local server, no authentication is required.

Select the **Disconnect from server after update** option if connection to the server remains active even after updates have been downloaded.

4.3.2 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking Update from the main menu.

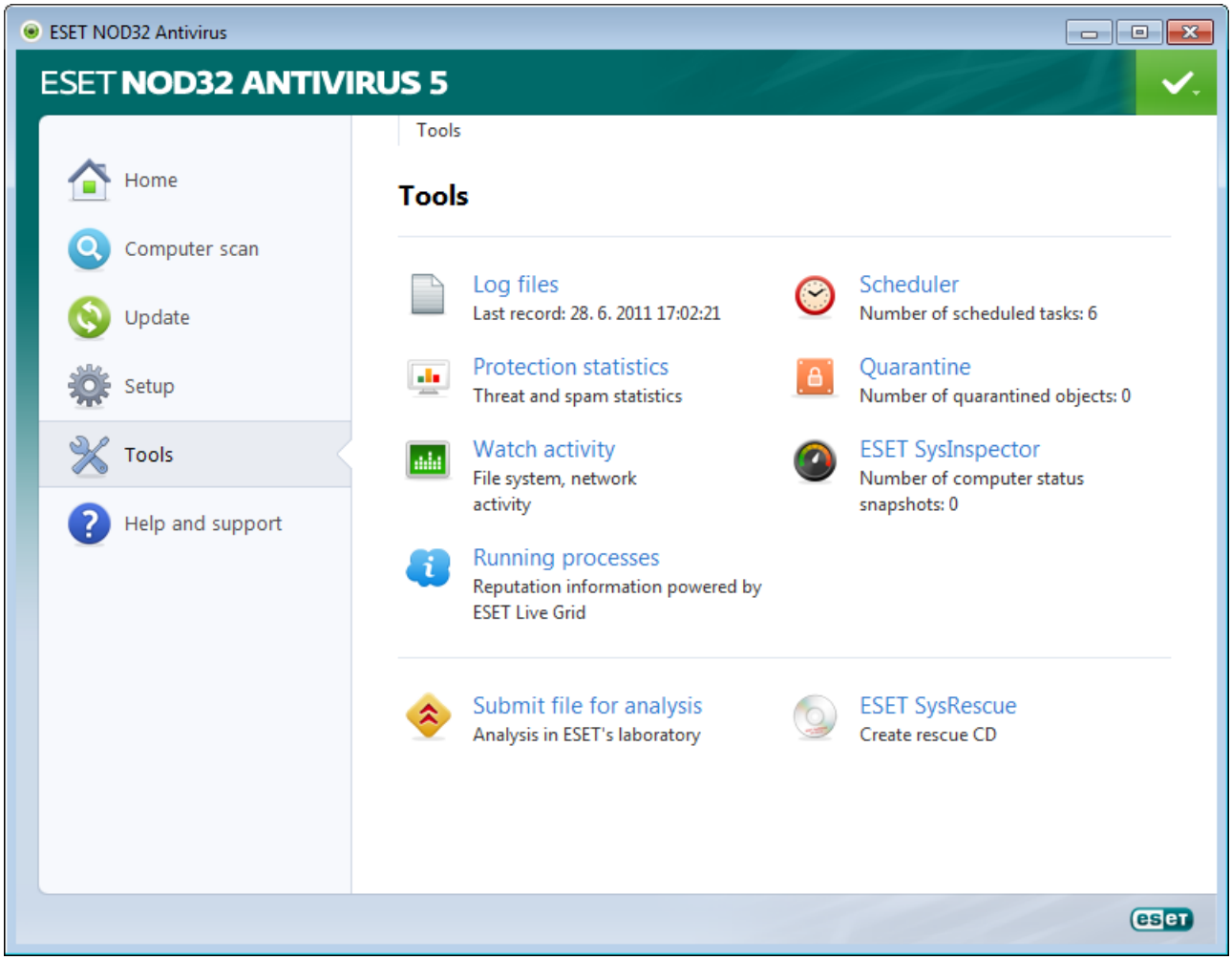
Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET NOD32 Antivirus:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see section Scheduler.

4.4 Tools

The **Tools** menu includes modules that help simplify program administration and offer additional options for advanced users.



This menu includes the following tools:

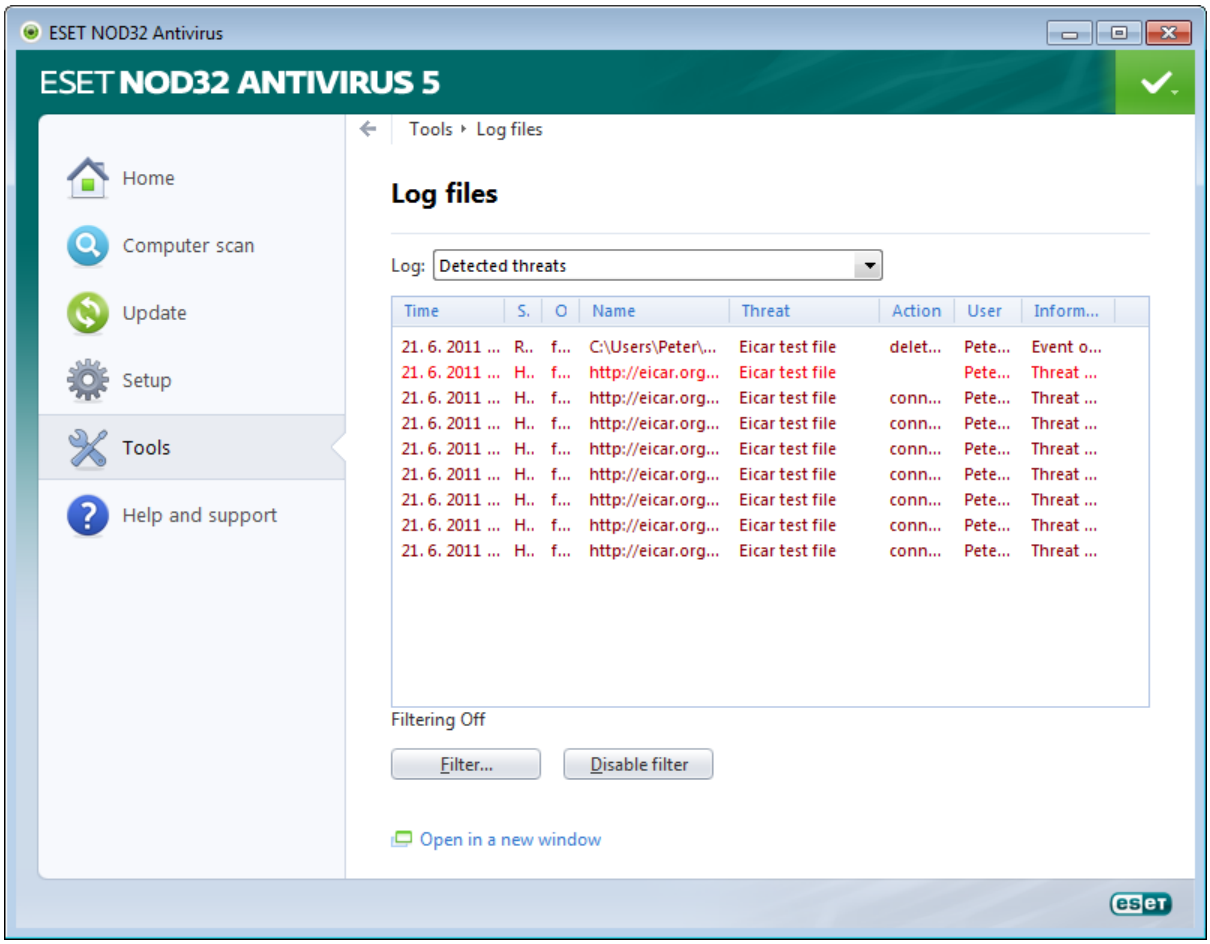
- Log files
- Protection statistics
- Watch activity
- Running processes
- Scheduler
- Quarantine
- ESET SysInspector

Submit file for analysis – Allows you to submit a suspicious file for analysis to ESET's Virus Lab. The dialog window displayed after clicking this option is described in the Submission of files for analysis section.

ESET SysRescue – Launches the ESET SysRescue creation wizard.

4.4.1 Log files

The Log files contain information about all important program events that have occurred and provide an overview of detected threats. Logging acts as an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view text messages and logs directly from the ESET NOD32 Antivirus environment, as well as to archive logs.



Log files are accessible from the main menu by clicking **Tools** > **Log files**. Select the desired log type using the **Log** drop-down menu at the top of the window. The following logs are available:

- **Detected threats** – The Threat log offers detailed information about infiltrations detected by ESET NOD32 Antivirus modules. The information includes the time of detection, name of infiltration, location, the performed action and the name of the user logged in at the time the infiltration was detected. Double-click the log entry to display its detailed content in a separate window.
- **Events** – All important actions performed by ESET NOD32 Antivirus are recorded in the Event logs. The Event log contains information about events and errors that have occurred in the program. It is designed for system administrators and users to solve problems Often the information found here can help you find a solution for a problem occurring in the program.
- **Computer scan** – Results of all completed manual or planned scans are displayed in this window. Each line corresponds to a single computer control. Double-click any entry to view details of the respective scan.
- **HIPS** – Contains records of specific rules which were marked for recording. The protocol shows the application that called the operation, the result (whether the rule was permitted or prohibited) and the created rule name.

In each section, the displayed information can be directly copied to the clipboard (keyboard shortcut Ctrl+C) by selecting the entry and clicking the **Copy** button. To select multiple entries, the CTRL and SHIFT keys can be used.

You can show the context menu by right-clicking on a specific record. From the context menu, you will have these options available:

- **Filter records of the same type** – After activating this filter, you will only see records of the same type (diagnostics, warnings, ...).
- **Filter.../Find...** – After clicking this option, a **Log filtering** window will pop up and you can define the filtering criteria.
- **Disable filter** – Clears all the settings made in the filter (as described above).
- **Copy all** – Copies information about all the records in the window.
- **Delete/Delete all** – Deletes the selected record(s) or all the records displayed – this action requires administrator privileges.
- **Export** – Exports information about the record(s) in XML format.
- **Scroll log** – Leave this option enabled to auto scroll old logs and watch active logs in the **Log files** window.

4.4.1.1 Log maintenance

The Logging configuration of ESET NOD32 Antivirus is accessible from the main program window. Click **Setup** > **Enter advanced setup...** > **Tools** > **Log files**. The logs section is used to define how the logs will be managed. The program automatically deletes older logs in order to save hard disk space. You can specify the following options for log files:

Delete records automatically – The log entries older than the specified number of days in **Delete records older than X days** will be automatically deleted.

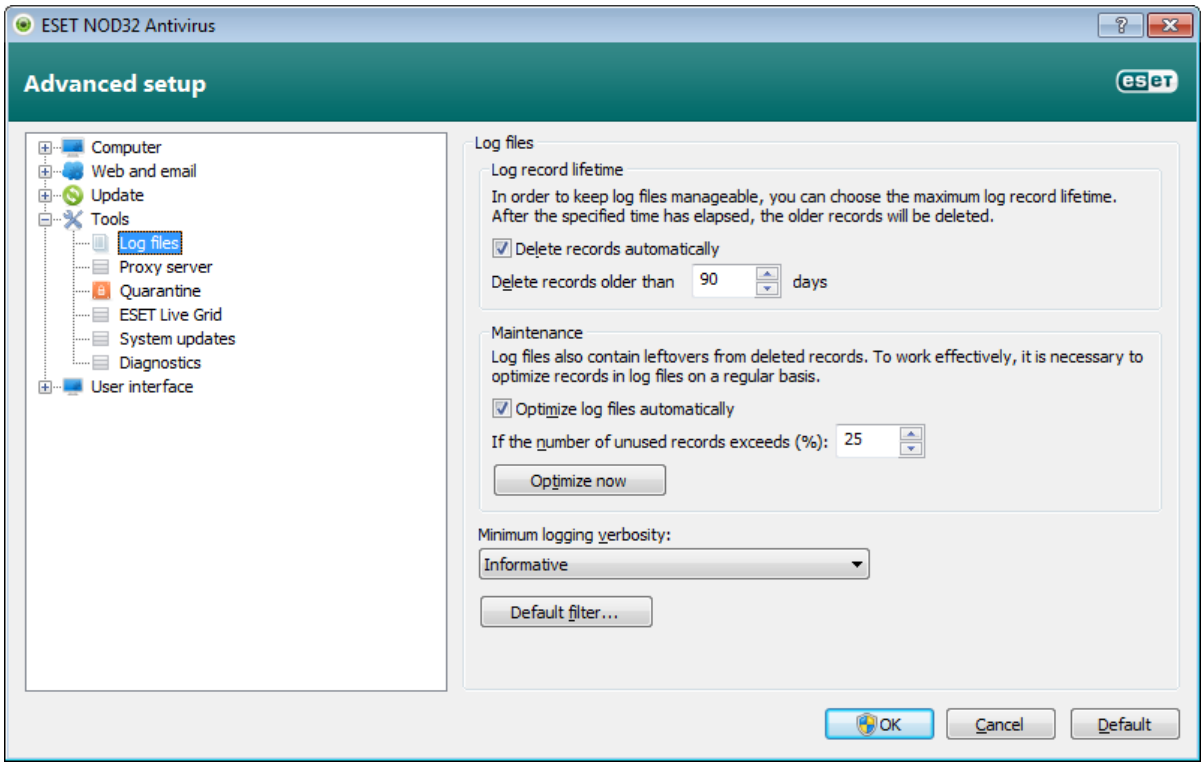
Optimize log files automatically – If checked, the log files will be automatically be defragmented if the percentage is higher than specified in **If the number of unused records exceeds (%)** value.

Click **Optimize now** to start the defragmenting the log files. All empty log entries are removed during this process, which improves performance and speed when processing the logs. This improvement can be observed especially if the logs contain a large number of entries.

Minimum logging verbosity – Specifies the minimum verbosity level of events to be logged.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as *"Error downloading file"* and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting Antivirus protection, etc...).

Click the **Default filter...** button to open the Log filtering window. Check record types to be displayed in logs and click **OK**.

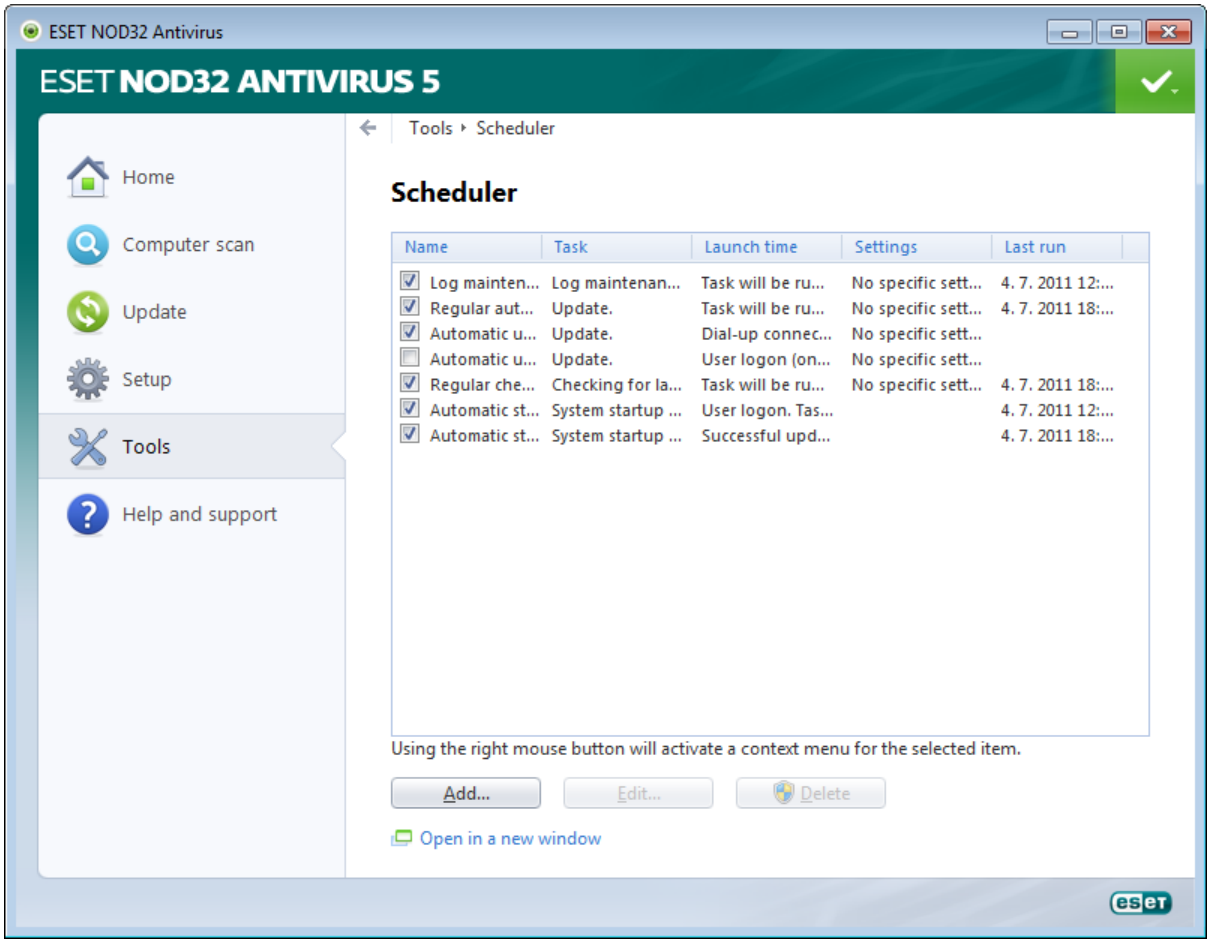


4.4.2 Scheduler

Scheduler manages and launches scheduled tasks with predefined configuration and properties.

The Scheduler can be accessed from the ESET NOD32 Antivirus main menu under **Tools**. The **Scheduler** contains a list of all scheduled tasks and configuration properties such as the predefined date, time and scanning profile used.

The Scheduler serves to schedule the following tasks: virus signature database update, scanning task, system startup file check and log maintenance. You can add or delete tasks directly from the main Scheduler window (click **Add...** or **Delete** at the bottom). Right click anywhere in the Scheduler window to perform the following actions: display detailed information, perform the task immediately, add a new task, and delete an existing task. Use the checkboxes at the beginning of each entry to activate/deactivate the tasks.



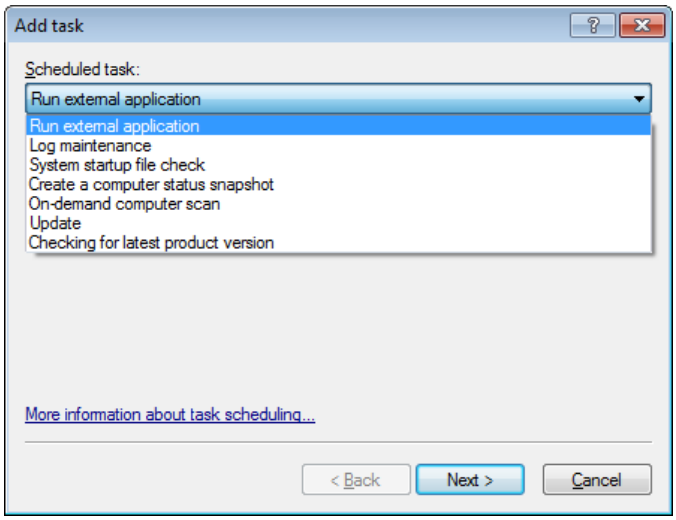
By default, the following scheduled tasks are displayed in **Scheduler**:

- **Log maintenance**
- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Regular checking for latest product version**
- **Automatic startup file check** (after user logon)
- **Automatic startup file check** (after successful update of the virus signature database)

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit...** or select the desired task you wish to modify and click the **Edit...** button.

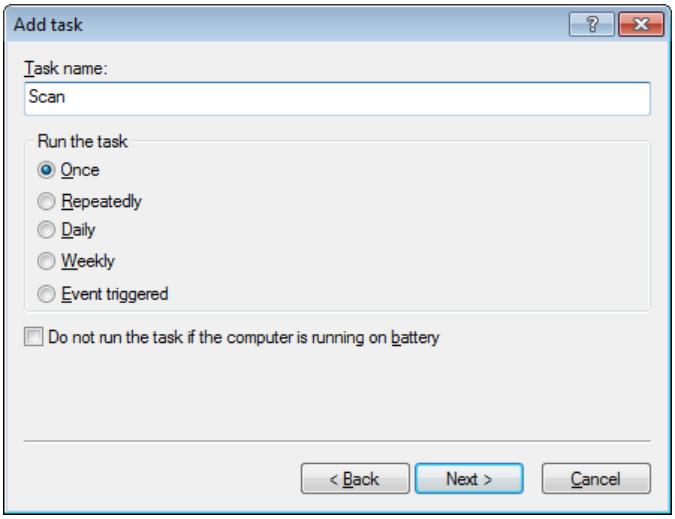
Add a new task

1. Click on **Add...** at the bottom of the window.
2. Select the desired task from the pull-down menu.



3. Enter the name of the task and select one from the timing options:

   - **Once** – The task will be performed only once, at the predefined date and time.
   - **Repeatedly** – The task will be performed at the specified interval (in hours).
   - **Daily** – The task will run each day at the specified time.
   - **Weekly** – The task will run once or more times a week, on the selected day(s) and time.
   - **Event triggered** – The task will be performed on a specified event.



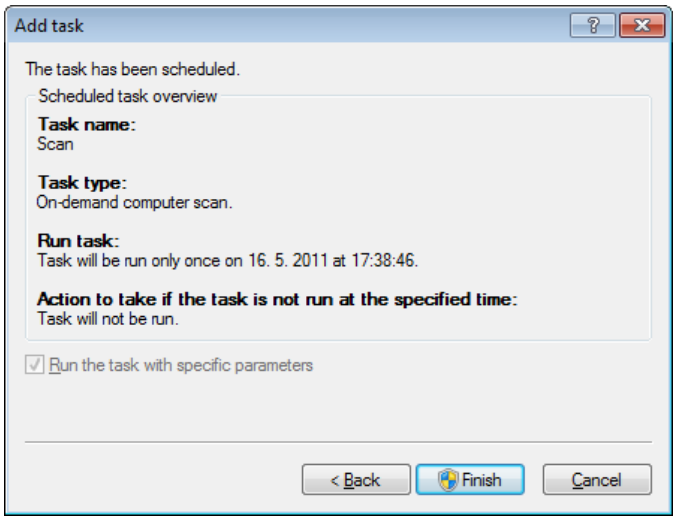
4. Depending on the timing option you choose in the previous step, one of the following dialog windows will be displayed:

   - **Once** – The task will be performed at the predefined date and time.
   - **Repeatedly** – The task will be performed at the specified time interval.
   - **Daily** – The task will run repeatedly each day at the specified time.
   - **Weekly** – The task will be run on the selected day and time.

5. If the task could not be run at the predefined time, you can specify when it will be performed again:

   - Wait until the next scheduled time
   - Run the task as soon as possible
   - Run the task immediately if the time since the last task execution exceeds -- hours

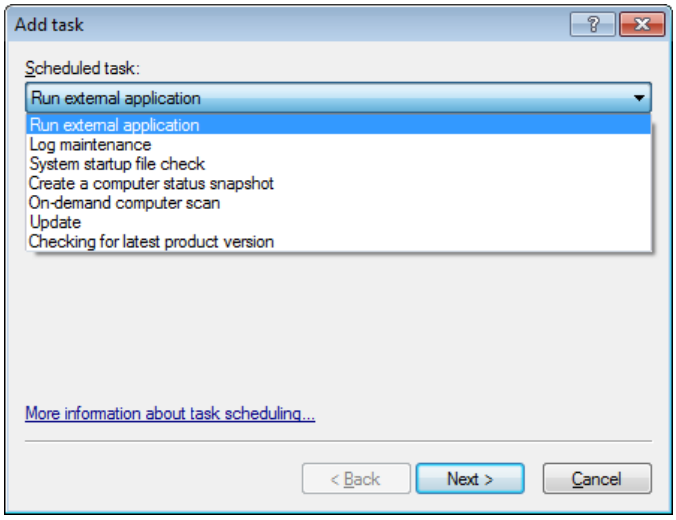
6. In the last step you can review the task to be scheduled. Click **Finish** to apply the task.


Add task
The task has been scheduled.
Scheduled task overview
Task name:
Scan
Task type:
On-demand computer scan.
Run task:
Task will be run only once on 16. 5. 2011 at 17:38:46.
Action to take if the task is not run at the specified time:
Task will not be run.
Run the task with specific parameters
< Back
Finish
Cancel

4.4.2.1 Creating new tasks

To create a new task in Scheduler, click the **Add...** button or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application** – Schedules the execution of an external application.
- **Log maintenance** – Log files also contains leftovers from deleted records. This task optimizes records in log files on a regular basis to work effectively.
- **System startup file check** – Checks files that are allowed to run at system startup or logon.
- **Create a computer status snapshot** – Creates the ESET SysInspector computer snapshot – gathers detailed information about system components (e.g. drivers, applications) and assesses the risk level of each component.
- **Computer scan** – Performs computer scan of files and folders on your computer.
- **Update** – Schedules an Update task by updating the virus signature database and by updating program modules.
- **Checking for latest product version**



Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task below.

From the **Scheduled task** drop-down menu, select **Update**. Click **Next** and enter the name of the task into the **Task name** field. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Use the **Do not run the task if the computer is running on battery** option to minimize system resources while a laptop is running on battery power. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

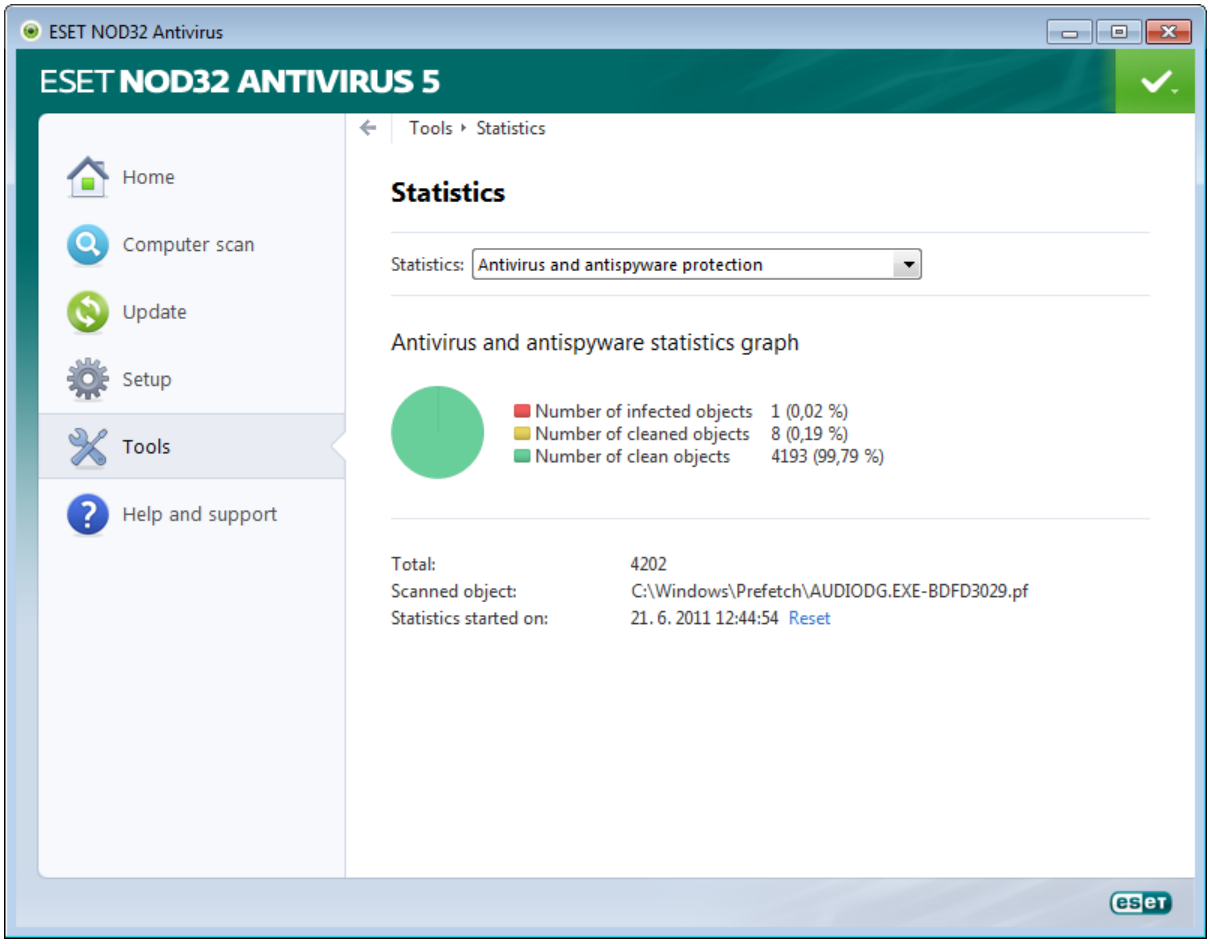
- **Wait until the next scheduled time**
- **Run task as soon as possible**
- **Run task immediately if the time since its last execution exceeds specified interval** (the interval can be defined using the Task interval scroll box)

In the next step, a summary window with information about the current scheduled task is displayed; the option **Run task with specific parameters** should be automatically enabled. Click the **Finish** button.

A dialog window will appear, allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternative profile, which is used if the task cannot be completed using the primary profile. Confirm by clicking **OK** in the **Update profiles** window. The new scheduled task will be added to the list of currently scheduled tasks.

4.4.3 Protection statistics

To view a graph of statistical data related to ESET NOD32 Antivirus's protection modules, click **Tools** > **Protection statistics**. Select the desired protection module from the **Statistics** drop-down menu to see the corresponding graph and legend. If you mouse over an item in the legend, only the data for that item will display in the graph.



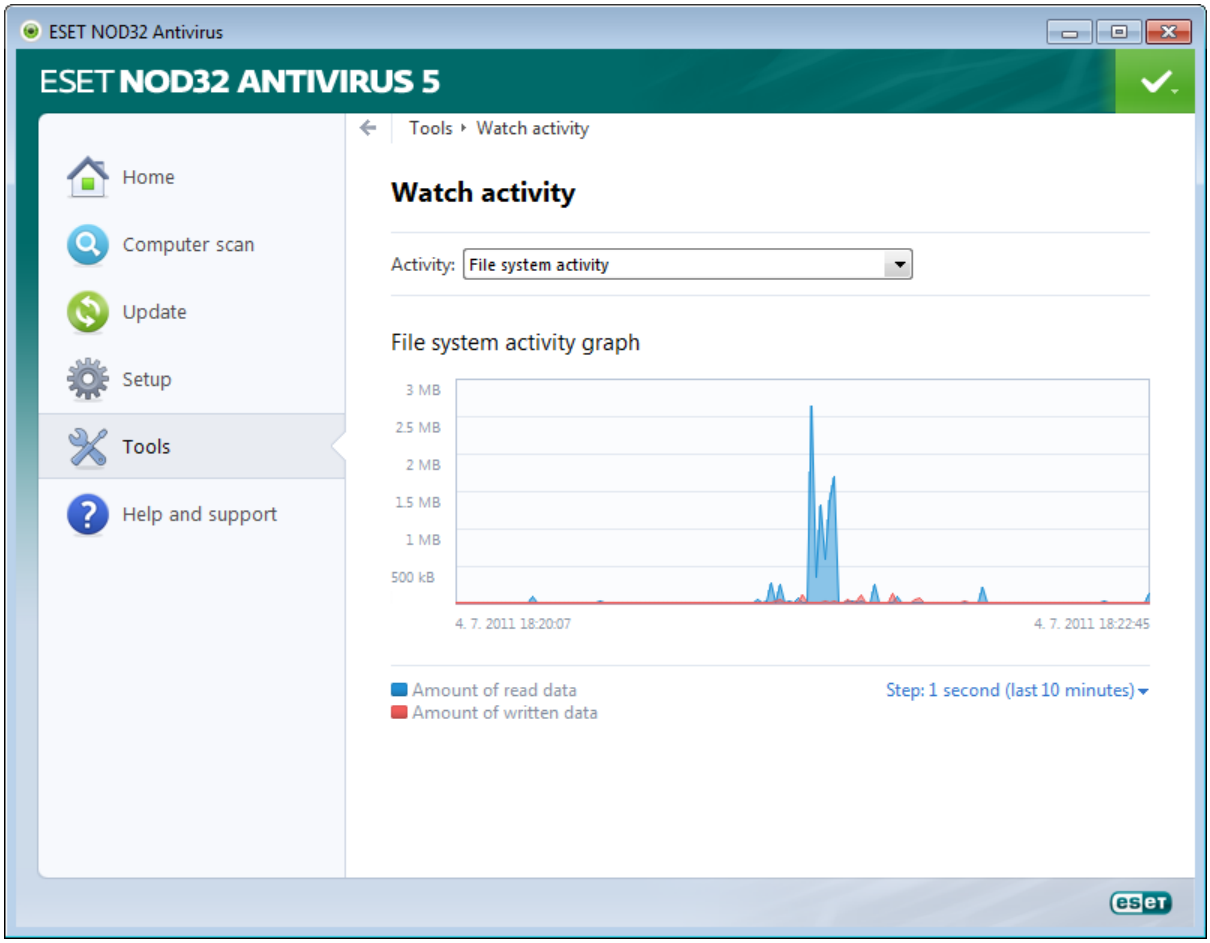
The following statistic graphs are available:

- **Antivirus and Antispyware protection** – Displays the number of infected and cleaned objects.
- **Real-time file system protection** – Only displays objects that were read or written to the file system.
- **Email client protection** – Only displays objects that were sent or received by email clients.
- **Web access protection** – Only displays objects downloaded by web browsers.

Below the statistics graphs, you can see the number of total scanned objects, latest scanned object and the statistics timestamp. Click **Reset** to clear all statistics information.

4.4.4 Watch activity

To see the current **File system activity** in graph form, click **Tools** > **Watch activity**. At the bottom of the graph is a timeline which records File system activity in real time based on the selected time span. To change the time span, click the **Step 1...** option located at the bottom-right of the window.



The following options are available:

- **Step 1 second (last 10 minutes)** – The graph refreshes every second and the timeline covers the last 10 minutes
- **Step 1 minute (last 24 hours)** – The graph is refreshed every minute and the timeline covers the last 24 hours
- **Step 1 hour (last month)** – The graph is refreshed every hour and the timeline covers the last month
- **Step 1 hour (selected month)** – The graph is refreshed every hour and the timeline covers the last X selected months

The vertical axis of the **File system activity graph** represents read data (red) and written data (blue). Both values are given in kilobytes. If you mouse over either read data or written data in the legend below the graph, the graph will only display data for that activity type.

4.4.5 ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and gathers detailed information about system components, such as installed drivers and applications, network connections or important registry entries and assesses the risk level of each component. The information can help determine the cause of suspicious system behavior that may be due to software or hardware incompatibility or malware infection.

The SysInspector window displays the following information about created logs:

- **Time** – The time of log creation.
- **Comment** – A short comment.
- **User** – The name of the user who created the log.
- **Status** – The status of log creation.

The following actions are available:

- **Compare** – Compares two existing logs.
- **Create...** – Creates a new log. Please wait until the ESET SysInspector log is complete (**Status** shown as Created).
- **Delete** – Removes selected logs from the list.

After right-clicking one or more selected logs, the following additional options are available from the context menu:

- **Show** – Opens the selected log in ESET SysInspector (same function as double-clicking a log).
- **Delete all** – Deletes all logs.
- **Export...** – Exports the log to an xml file or zipped xml.

4.4.6 ESET Live Grid

ESET Live Grid (the next generation of ESET ThreatSense.Net) is an advanced warning system against emerging threats based on reputation. Utilizing real-time streaming of threat-related information from the cloud, ESET virus lab keeps the defenses up-to-date for a constant level of protection. User can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET Live Grid. There are two options:

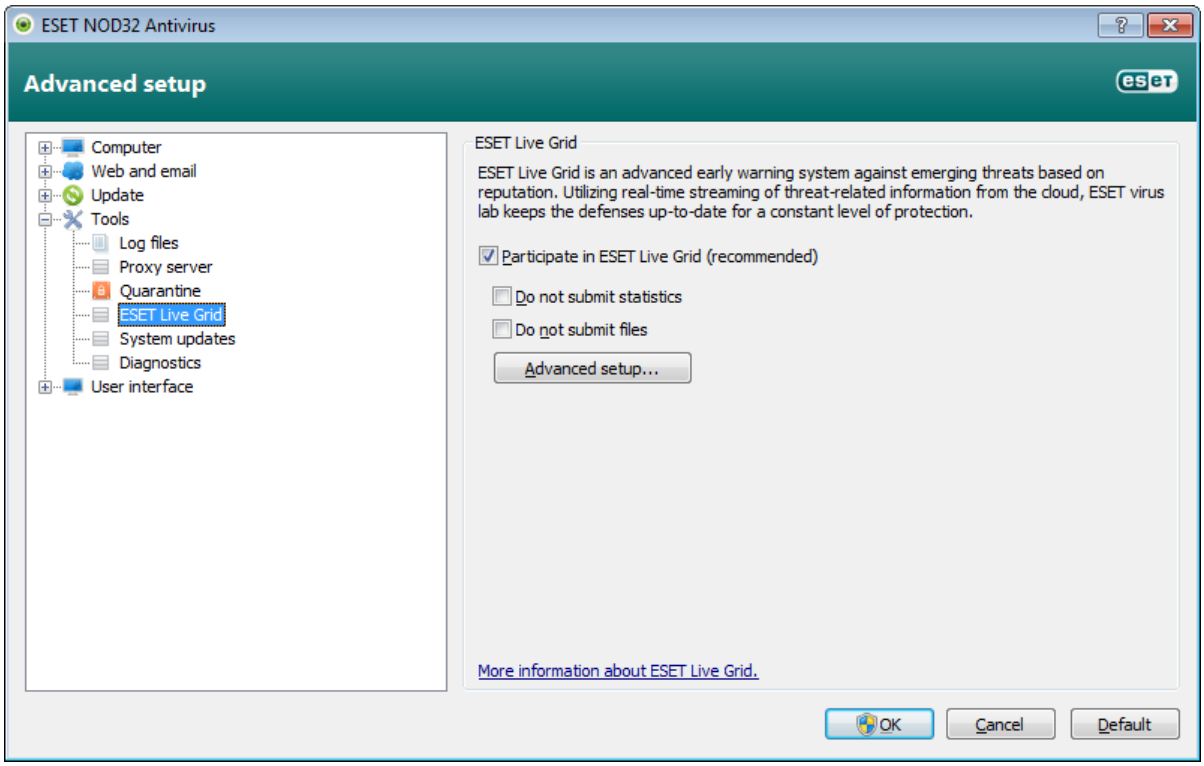
1. You can decide to not enable the ESET Live Grid. You will not lose any functionality in the software, and you will still receive the best protection that we offer.
2. You can configure the ESET Live Grid to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

The ESET Live Grid will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer's operating system.

While there is a chance that this may occasionally disclose some information about you or your computer (usernames in a directory path, etc.) to ESET's Virus Lab, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

By default, ESET NOD32 Antivirus is configured to ask before submitting suspicious files for detailed analysis to ESET's Virus Lab. Files with certain extensions such as *.doc* or *.xls* are always excluded. You can also add other extensions if there are particular files that you or your organization wants to avoid sending.

The ESET Live Grid's setup menu provides several options for enabling / disabling the ESET Live Grid that serves to submit suspicious files and anonymous statistical information to ESET's labs. It is accessible from the Advanced Setup tree, under **Tools** > **ESET Live Grid**.



Participate in ESET Live Grid (recommended) – Enables / disables the ESET Live Grid that serves to submit suspicious files and anonymous statistical information to ESET's labs.

Do not submit statistics – Select this option if you do not wish to submit anonymous information from the ESET Live Grid about your computer. This information is related to newly detected threats, which may include the name of the infiltration, information about the date and time it was detected, the version of ESET NOD32 Antivirus, information about your computer's operating system version and Location settings. The statistics are normally delivered to ESET's server once or twice a day.

Do not submit files – Suspicious files, resembling infiltrations in their content or behavior, are not submitted to ESET for analysis by means of ESET Live Grid technology.

Advanced setup... – Opens a window with further ESET Live Grid settings.

If you have used the ESET Live Grid before and have disabled it, there still may be data packages to send. Even after deactivating, such packages will be sent to ESET on the next occasion. Afterwards, no further packages will be created.

4.4.6.1 Suspicious files

The **Files** tab in ESET Live Grid advanced setup allows you to configure how threats are submitted to ESET's Virus Lab for analysis.

If you find a suspicious file, you can submit it for analysis to our ThreatLabs. If it is a malicious application, its detection will be added to the next virus signature update.

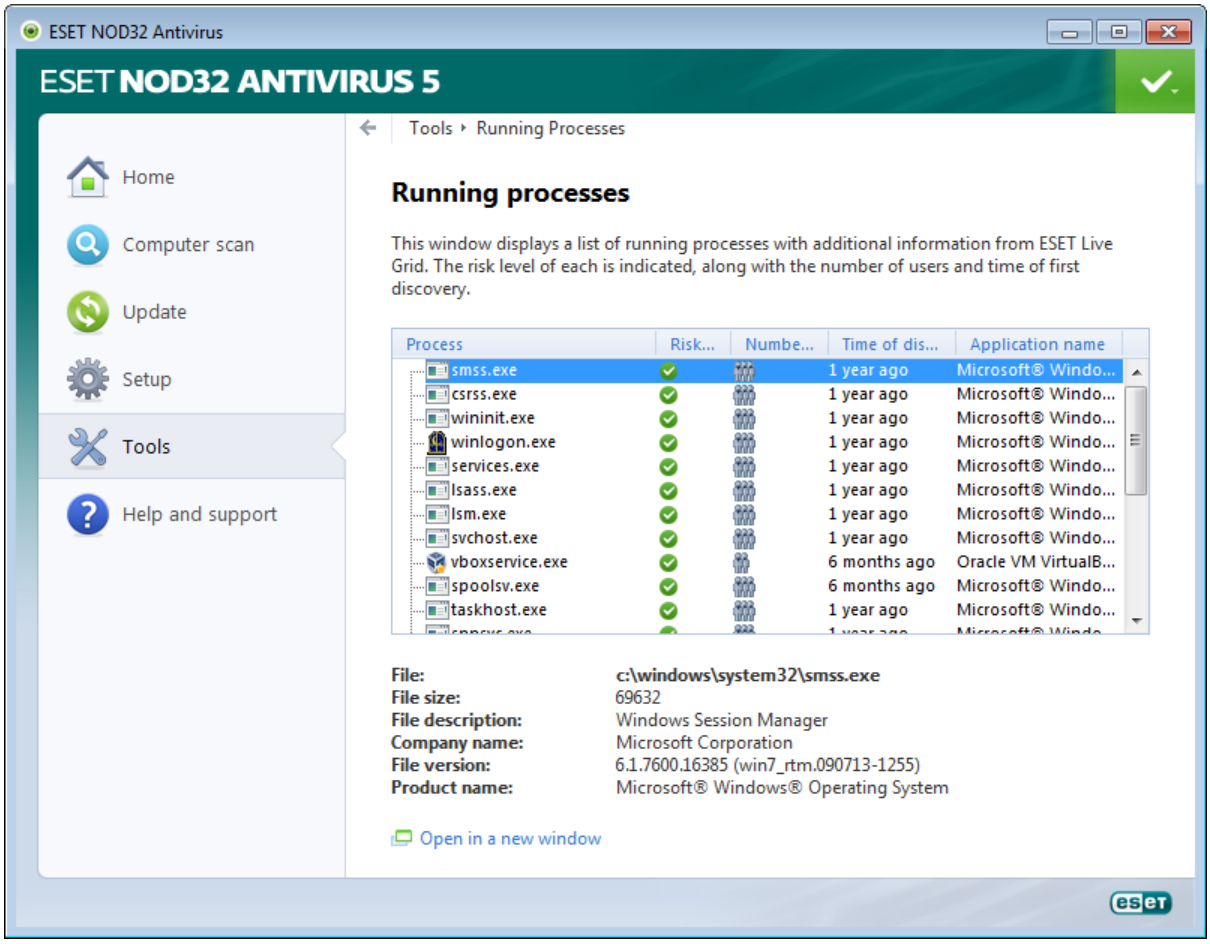
Exclusion filter – The Exclusion filter allows you to exclude certain files/folders from submission. The files listed will never be sent to ESET's labs for analysis, even if they contain a suspicious code. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

Contact email (optional) – Your contact email can be included with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

Select the **Enable logging** option to create a event log to record file and statistical information submissions. It enables logging to the Event log when files or statistics are sent.

4.4.7 Running processes

Reputation of Running processes displays the running programs or processes on your computer and keeps ESET immediately and continuously informed about new infiltrations. ESET NOD32 Antivirus provides detailed information on running processes to protect users with ESET Live Grid technology.


ESET NOD32 Antivirus
ESET NOD32 ANTIVIRUS 5
Home
Computer scan
Update
Setup
Tools
Help and support
Tools ‣ Running Processes
Running processes
This window displays a list of running processes with additional information from ESET Live Grid. The risk level of each is indicated, along with the number of users and time of first discovery.
Process
Risk...
Numbe...
Time of dis...
Application name
smss.exe 1 year ago Microsoft® Windo...
csrss.exe 1 year ago Microsoft® Windo...
wininit.exe 1 year ago Microsoft® Windo...
winlogon.exe 1 year ago Microsoft® Windo...
services.exe 1 year ago Microsoft® Windo...
lsass.exe 1 year ago Microsoft® Windo...
lsm.exe 1 year ago Microsoft® Windo...
svchost.exe 1 year ago Microsoft® Windo...
vboxservice.exe 6 months ago Oracle VM VirtualB...
spoolsv.exe 6 months ago Microsoft® Windo...
taskhost.exe 1 year ago Microsoft® Windo...
File: c:\windows\system32\smss.exe
File size: 69632
File description: Windows Session Manager
Company name: Microsoft Corporation
File version: 6.1.7600.16385 (win7_rtm.090713-1255)
Product name: Microsoft® Windows® Operating System
Open in a new window
eset

Process – Image name of the program or process that is currently running on your computer. You can also use the Windows Task Manager to see all running processes on your computer. You can open Task Manager by right-clicking an empty area on the taskbar and then clicking Task Manager, or by pressing Ctrl+Shift+Esc on your keyboard.

Risk – In most cases, ESET NOD32 Antivirus, using ESET Live Grid technology, assigns risk levels to objects (files, processes, registry keys, etc.) using a series of heuristic rules that examine the characteristics of each object and then weigh their potential for malicious activity. Based on these heuristics, objects are assigned a risk level from "1 – Fine (green)" to "9 – Risky (red)".

NOTE: Known applications marked as 1 – Fine (green) are definitely clean (white-listed) and will be excluded from scanning, as this will improve the scanning speed of on-demand computer scan or Real-time file system protection on your computer.

Users – The number of users that use a given application. This information are gathered by ESET Live Grid technology.

Discovered – Period of time since the application was discovered by ESET Live Grid technology.

NOTE: When an application is marked as 9 – Risky (red) security level, it is not necessarily malicious software. Usually it is just a newer application. If you are not sure about the file, you can Submit file for analysis to ESET's Virus Lab. If the file turns out to be a malicious application, its detection will be added in one of the upcoming updates.

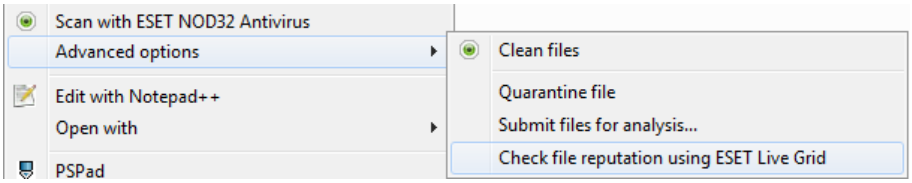
Name – The given name of a program or process.

Open in a new window – The Running processes information will be opened in a new window.

By clicking on a given application at the bottom, the following information will appear at the bottom of the window:

- **File** – Location of an application on your computer.
- **File size** – File size in KB (kilobytes).
- **File description** – File characteristics based on the description from the operating system.
- **Company name** – Name of the vendor or application process.
- **File version** – Information from the application publisher.
- **Product name** – Application name and/or business name.

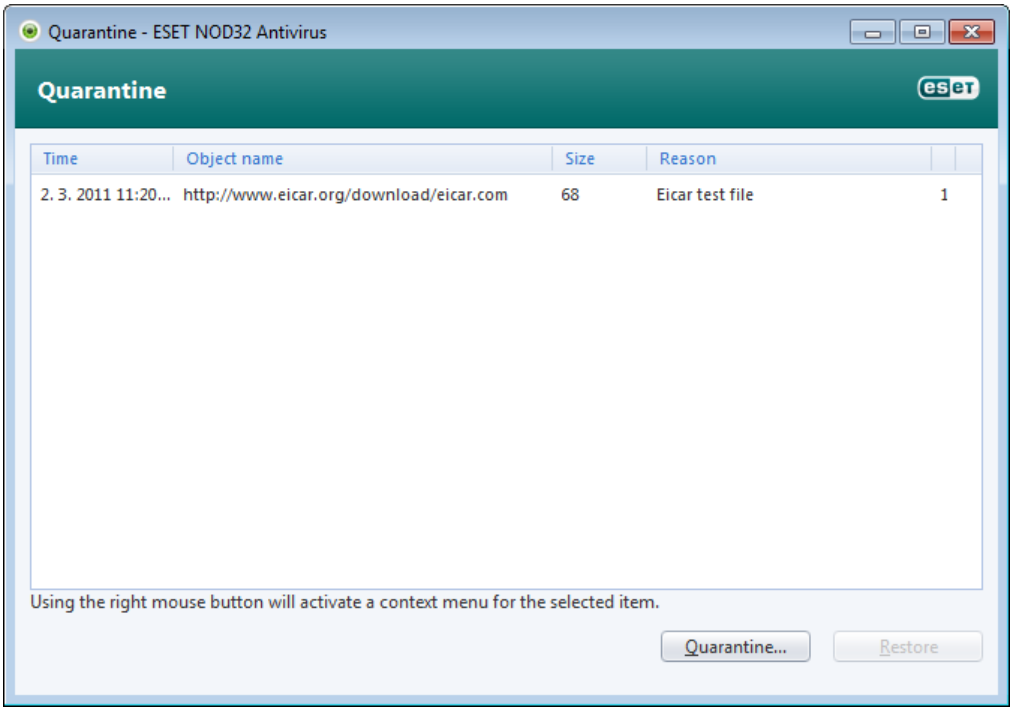
NOTE: Reputation can also be run on files that do not act as a running programs/processes – mark files you want to check, right-click on them and from the context menu select **Advanced options** > **Check File Reputation using ESET Live Grid**.



4.4.8 Quarantine

The main task of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET NOD32 Antivirus.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to ESET's Virus Lab.



Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (e.g. object added by user), and number of threats (e.g., if it is an archive containing multiple infiltrations).

4.4.8.1 Quarantining files

ESET NOD32 Antivirus automatically quarantines deleted files (if you have not cancelled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking the **Quarantine...** button. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose; right-click in the **Quarantine** window and select **Quarantine...**.

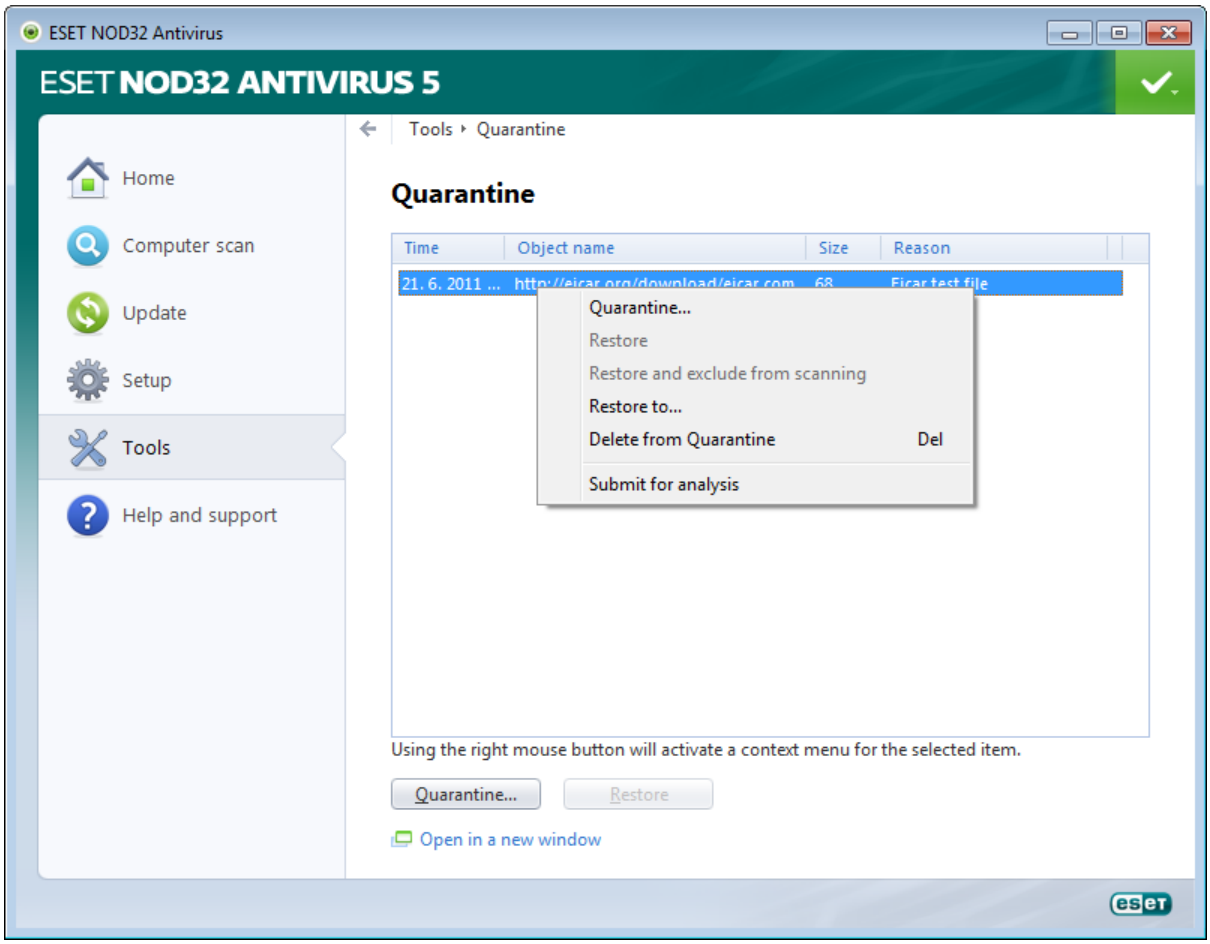
4.4.8.2 Restoring from Quarantine

Quarantined files can also be restored to their original location. Use the **Restore** feature for this purpose, which is available from the context menu by right-clicking on the given file in the Quarantine window. The context menu also offers the option **Restore to...**, which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

4.4.8.3 Submitting file from Quarantine

If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (e.g., by heuristic analysis of the code) and subsequently quarantined, please send the file to ESET's Virus Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.



4.4.9 Submission of files for analysis

The file submission dialog enables you to send a file to ESET for analysis and can be found in **Tools** > **Submit file for analysis**. If you find a suspiciously behaving file on your computer, you can submit it to ESET's Virus Lab for analysis. If the file turns out to be a malicious application, its detection will be added in one of the upcoming updates.

Alternatively, you can submit the file by email. If you prefer this option, pack the file(s) using WinRAR/ZIP, protect the archive with the password "infected" and send it to samples@eset.com. Please remember to use a descriptive subject and enclose as much information about the file as possible (e.g., the website you downloaded it from).

NOTE: Before submitting a file to ESET, make sure it meets either of the following criteria:
– the file is not detected at all,
– the file is incorrectly detected as a threat.
You will not receive a response unless further information is required for analysis.

Reason for submitting the file – Select the description that best fits your message. Choose from the following three options: **Suspicious file**, **False positive** and **Other**.

File – The path to the file you intend to submit.

Contact email – This contact email is sent along with suspicious files to ESET and may be used to contact you if further information is required for analysis. Entering a contact email is optional. You will not get a response from ESET unless more information is required, since each day our servers receive tens of thousands of files, which makes it impossible to reply to all submissions.

4.4.10 System updates

The Windows update feature is an important component of protecting users from malicious software. For this reason, it is vital to install Microsoft Windows updates as soon as they become available. ESET NOD32 Antivirus notifies you about missing updates according to the level you specify. The following levels are available:

- **No updates** – No system updates will be offered for download.
- **Optional updates** – Updates marked as low priority and higher will be offered for download.
- **Recommended updates** – Updates marked as common and higher will be offered for download.
- **Important updates** – Updates marked as important and higher will be offered for download.
- **Critical updates** – Only critical updates will be offered for download.

Click **OK** to save changes. The System updates window will be displayed after status verification with the update server. Accordingly, the system update information may not be immediately available after saving changes.

4.4.11 Diagnostics

Diagnostics provides application crash dumps of ESET's processes (e.g. *ekrn*). If an application crashes, a dump will be generated. This can help developers to debug and fix various ESET NOD32 Antivirus problems. Two available dump types are available:

- **Complete memory dump** – Records all the contents of system memory when application stops unexpectedly. A complete memory dump may contain data from processes that were running when the memory dump was collected.
- **Minidump** – Records the smallest set of useful information that may help identify why the application crashed unexpectedly. This kind of dump file can be useful when space is limited. However, because of the limited information included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.
- Select **Do not generate memory dump** (default) to disable this feature.

Target directory – Directory where the dump during the crash will be generated. Click **Open folder...** to open this directory within a new *Windows explorer* window.

4.5 User interface

The **User interface** section allows you to configure the behavior of the program's GUI (Graphical user interface).

Using the Graphics tool, you can adjust the program's visual appearance and effects used.

By configuring Alerts and notifications, you can change the behavior of detected threat alerts and system notifications. These can be customized to fit your needs.

If you choose not to display some notifications, they will be displayed in the Hidden notification windows area. Here you can check their status, show more details or remove them from this window.

To provide maximum security of your security software, you can prevent any unauthorized changes by protecting the settings by a password using the Access setup tool.

The Context menu is displayed after right-clicking on the selected object. Use this tool to integrate the ESET NOD32 Antivirus control elements into the context menu.

Gamer mode is useful for gamers and other users, who want to work with an application, and not be interrupted by pop-up windows, scheduled tasks and any components that could load the processor and RAM.

4.5.1 Graphics

The user interface configuration options in ESET NOD32 Antivirus allow you to adjust the working environment to fit your needs. These configuration options are accessible from the **User interface** > **Graphics** branch of the ESET NOD32 Antivirus Advanced Setup tree.

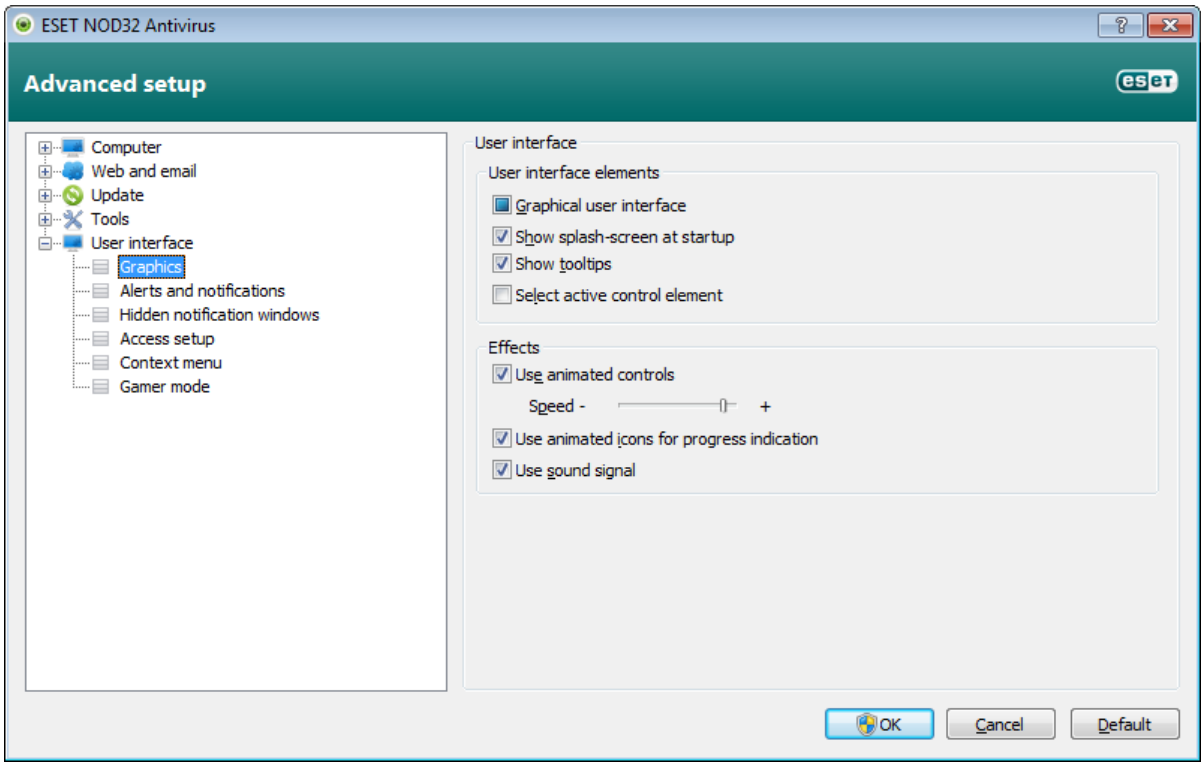
In the **User interface elements** section, the **Graphical user interface** option should be disabled if the graphical elements slow the performance of your computer or cause other problems. The graphical interface may also need to be turned off for visually impaired users, as it may conflict with special applications that are used for reading text displayed on the screen.

If you wish to deactivate the ESET NOD32 Antivirus splash-screen, deselect the **Show splash-screen at startup** option.

If the **Show tooltips** option is enabled, a short description of any option will be displayed if the cursor is placed over the option. The **Select active control element** option will cause the system to highlight any element which is currently under the active area of the mouse cursor. The highlighted element will be activated after a mouse click.

To decrease or increase the speed of animated effects, select the **Use animated controls** option and move the **Speed** slider bar to the left or right.

To enable the use of animated icons to display the progress of various operations, select the **Use animated icons for progress indication** option. If you want the program to sound a warning if an important event takes place, select the **Use sound signal** option.



4.5.2 Alerts and notifications

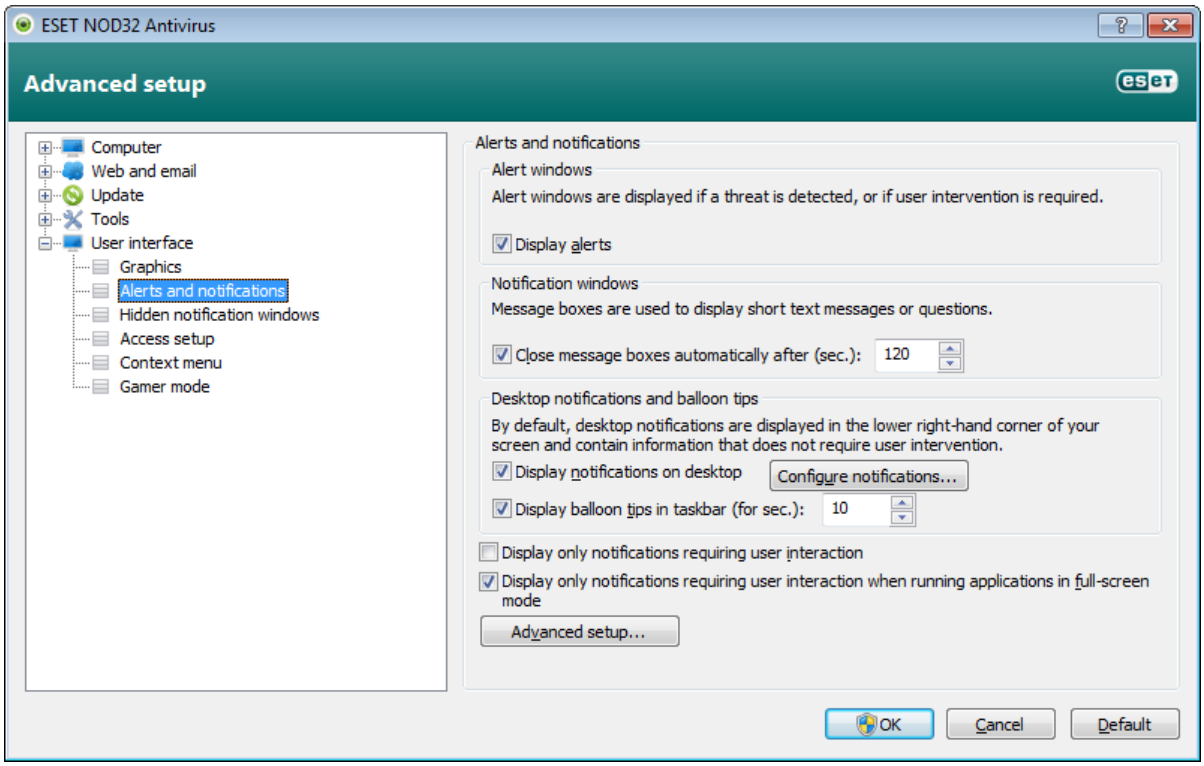
The **Alerts and notifications setup** section under **User interface** allows you to configure how threat alerts and system notifications (e.g. successful update messages) are handled in ESET NOD32 Antivirus. You can also set display time and the level of transparency of system tray notifications (it applies only to the systems supporting system tray notifications).

The first item is **Display alerts**. Disabling this option will cancel all alert windows and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left to its default setting (enabled).

To close pop-up windows automatically after a certain period of time, select the option **Close messageboxes automatically after (sec.)**. If they are not closed manually, alert windows are automatically closed after the specified time period has expired.

Notifications on the Desktop and balloon tips are informative only, and do not require or offer user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate Desktop notifications, select the **Display notifications on desktop** option. More detailed options, such as notification display time and window transparency can be modified by clicking the **Configure notifications...** button. To preview the behavior of notifications, click the **Preview** button.

To configure the duration of the balloon tips display time, see the option **Display balloon tips in taskbar (for sec.)**.


ESET NOD32 Antivirus
Advanced setup
eset
Computer
Web and email
Update
Tools
User interface
Graphics
Alerts and notifications
Hidden notification windows
Access setup
Context menu
Gamer mode
Alerts and notifications
Alert windows
Alert windows are displayed if a threat is detected, or if user intervention is required.
Display alerts
Notification windows
Message boxes are used to display short text messages or questions.
Close message boxes automatically after (sec.): 120
Desktop notifications and balloon tips
By default, desktop notifications are displayed in the lower right-hand corner of your screen and contain information that does not require user intervention.
Display notifications on desktop
Configure notifications...
Display balloon tips in taskbar (for sec.): 10
Display only notifications requiring user interaction
Display only notifications requiring user interaction when running applications in full-screen mode
Advanced setup...
OK
Cancel
Default

The **Display only notifications requiring user's interaction** option allows you to toogle alerts and notifications that require no user interaction. Select **Display only notifications requiring user's interaction when running applications in full screen mode** to suppress all noninteractive notifications.

Click **Advanced setup...** to enter additional **Alerts and notification** setup options.

4.5.2.1 Advanced setup

From the **Minimum verbosity of events to display** drop-down menu, you can select the starting severity level of alerts and notification to be displayed.

- **Diagnostic** – Logs information needed to fine-tune the program and all records above.
- **Informative** – Records informative messages, including successful update messages, plus all records above.
- **Warnings** – Records critical errors and warning messages.
- **Errors** – Errors such as *"Error downloading file"* and critical errors will be recorded.
- **Critical** – Logs only critical errors (error starting Antivirus protection, etc...).

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems, display notifications on the screen of this user** field specifies a user who will receive system and other notifications on systems allowing more users to connect at the same time. Normally this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

4.5.3 Hidden notification windows

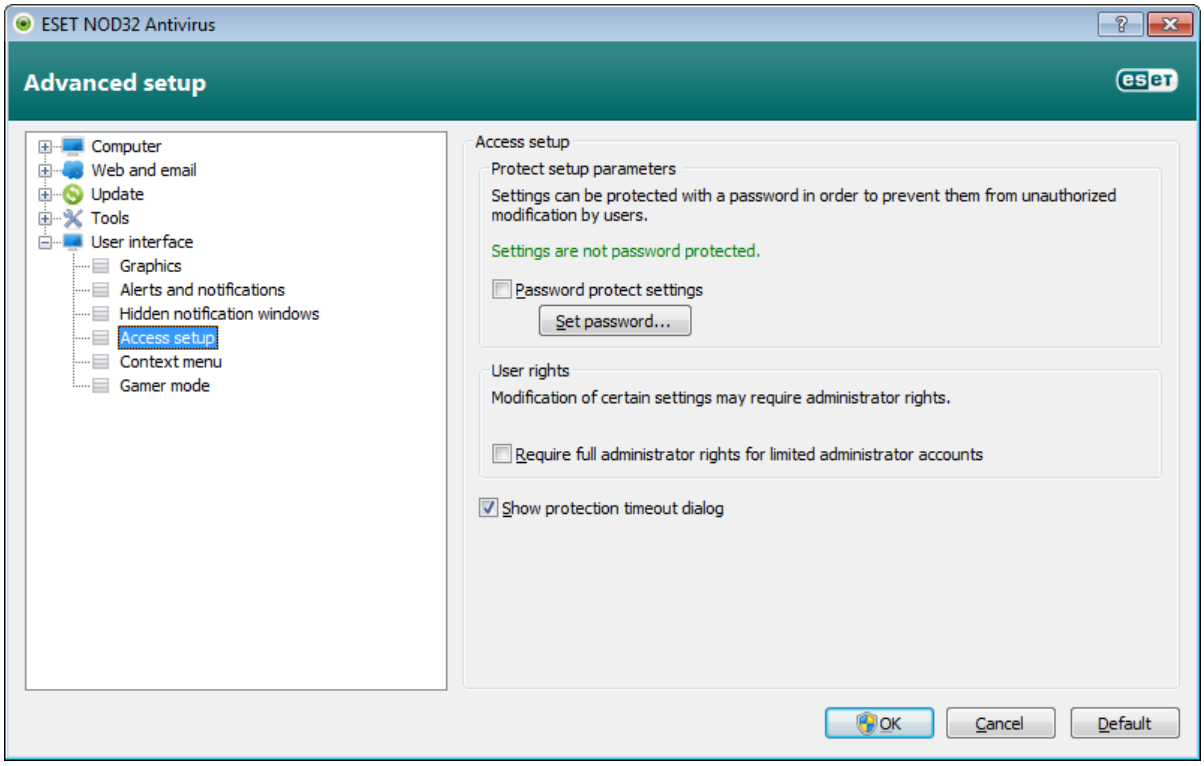
If the **Do not show this message again** option was selected for any notification window (alert) which was previously displayed, it will appear in the list of hidden notification windows. Actions that are now executed automatically are displayed in the column titled **Confirm**.

Show – Shows a preview of notification windows that are currently not displayed and for which an automatic action is configured.

Remove – Removes items from the **Hidden messageboxes** list. All notification windows removed from the list will be displayed again.

4.5.4 Access setup

In order to provide maximum security for your system, it is essential for ESET NOD32 Antivirus to be correctly configured. Any unqualified change may result in a loss of your important data. This option is located in the **Access setup** submenu under **User interface**. To avoid unauthorized modifications, the setup parameters of ESET NOD32 Antivirus can be password protected.



Password protect settings – Locks/unlocks the program's setup parameters. Check or uncheck the checkbox to open the Password setup window.

To set or change a password to protect the setup parameter, click **Set password...**.

Require full administrator rights for limited administrator accounts – Select this option to prompt the current user (if he or she does not have administrator rights) to enter administrator username and password when modifying certain system parameters (similar to the UAC in Windows Vista). The modifications include disabling protection modules.

Show protection timeout dialog – You will be prompted if this option is selected while temporarily disabling the protection from program menu or via **ESET NOD32 Antivirus** > **Setup** section. A **Time interval** drop-down menu in **Temporarily disable protection** window represents the period of time all selected parts of protection will be disabled.

4.5.5 Context menu

The context menu is displayed after right-clicking on the selected object. The menu lists all options available to perform on the object.

It is possible to integrate the ESET NOD32 Antivirus control elements into the context menu. More detailed setup options for this functionality is available in advanced options, in the sections **User Interface** and **Context menu**.

Integrate into the context menu – Integrate the ESET NOD32 Antivirus control elements into the context menu.

The following options are available in the **Menu type** drop-down menu:

- **Full (scan first)** – Activates all context menu options; the main menu will display the **Scan with ESET NOD32 Antivirus option**.
- **Full (clean first)** – Activates all context menu options; the main menu will display the **Clean with ESET NOD32 Antivirus option**.
- **Only scan** – Only the **Scan with ESET NOD32 Antivirus** option will be displayed in the context menu.
- **Only clean** – Only the **Clean with ESET NOD32 Antivirus** option will be displayed in the context menu.

Confirmations – Displays an additional warning when the user attempts to apply a context menu option on more objects than specified in **Ask if the number of files exceeds**. By default this option is set to eight objects.

4.5.6 Gamer mode

Gamer mode is a feature for gamers that demand uninterrupted usage of their software, do not wish to be disturbed by pop-up windows and want to minimize CPU usage. Gamer mode can also be used as a presentation mode, when a presentation cannot be interrupted by antivirus activity. By enabling this feature, all pop-up windows are disabled and the activity of the scheduler will be completely stopped. System protection still runs in the background but does not demand any user interaction.

You can enable or disable Gamer mode in the ESET NOD32 Antivirus main window in the **Setup** pane on the right side, or after entering the advanced setup menu. You can enter the advanced setup menu by clicking the **Enter advanced setup...** option at the bottom of the main program window, then selecting **User Interface** > **Gamer mode**. Select the **Enable Gamer mode** checkbox on the right side to enable this feature. Enabling Gamer mode is a potential security risk, so the protection status icon on the taskbar will turn yellow with a warning. You can also see this warning in the ESET NOD32 Antivirus main window in the **Home** pane, where you will find **Gamer mode enabled**, in yellow.

By selecting the **Enable Gamer mode when running applications in full screen automatically** checkbox, Gamer mode will start after you start a full-screen application and will automatically stop after you exit the application. This is especially useful for starting Gamer mode directly after starting a game, opening a full screen application or starting a presentation.

You can also select the **Disable Gamer mode automatically after X minutes** by selecting the checkbox and defining the amount of time (default value is 1 minute). This is used if you only require Gamer mode for a specific amount of time and want to automatically disable it afterwards.

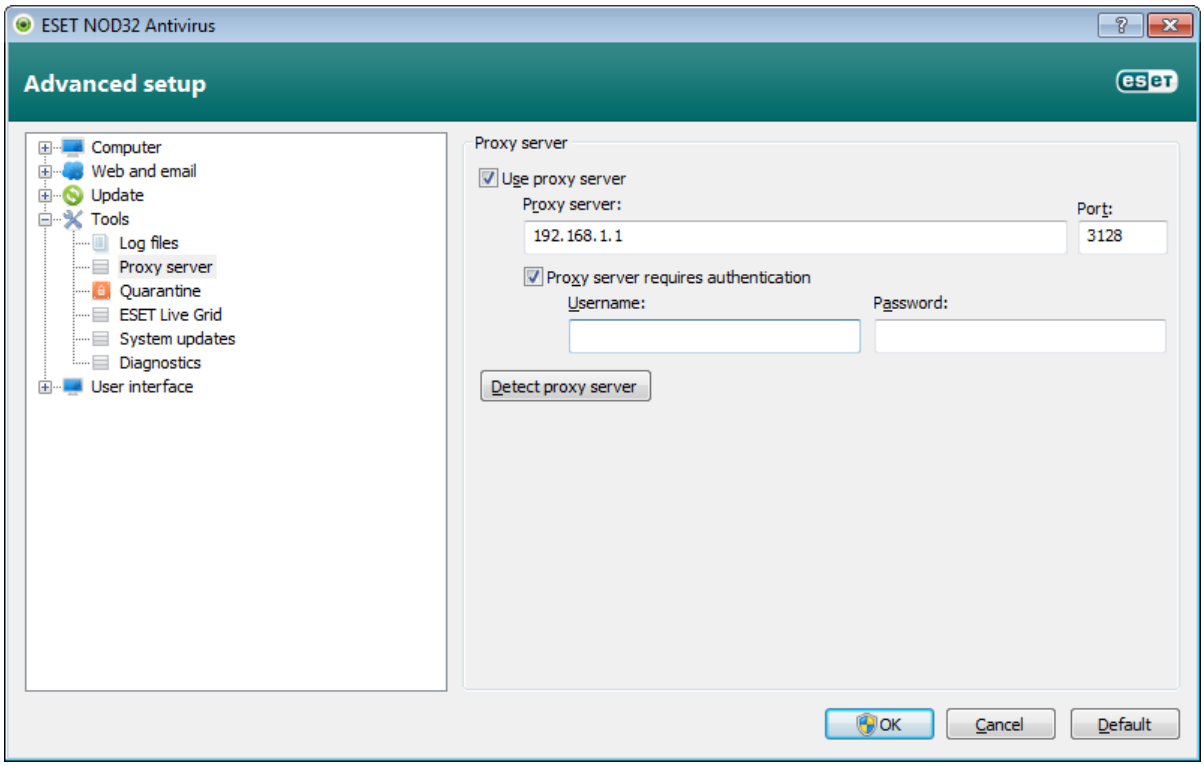
5. Advanced user

5.1 Proxy server setup

In large LAN networks, the connection of your computer to the Internet can be mediated by a proxy server. If this is the case, the following settings need to be defined. Otherwise the program will not be able to update itself automatically. In ESET NOD32 Antivirus, proxy server setup is available in two different sections within the Advanced Setup tree.

First, proxy server settings can be configured in **Advanced setup** under **Tools** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET NOD32 Antivirus. Parameters here will be used by all modules requiring connection to the Internet.

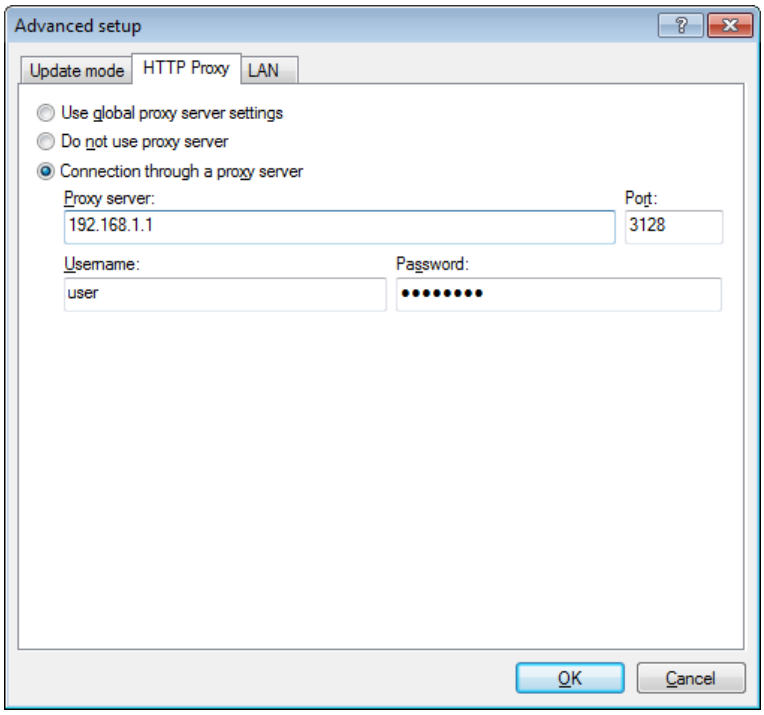
To specify proxy server settings for this level, select the **Use proxy server** checkbox and then enter the address of the proxy server into the **Proxy server** field, along with the **Port** number of the proxy server.



If communication with the proxy server requires authentication, select the **Proxy server requires authentication** checkbox and enter a valid **Username** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied.

NOTE: This feature does not retrieve authentication data (username and password); it must be supplied by you.

Proxy server settings can also be established within Advanced update setup (**Update** branch of the **Advanced Setup** tree). This setting applies for the given update profile and is recommended for laptops, as they often receive virus signature updates from different locations. For more information about this setting, see section Advanced update setup.



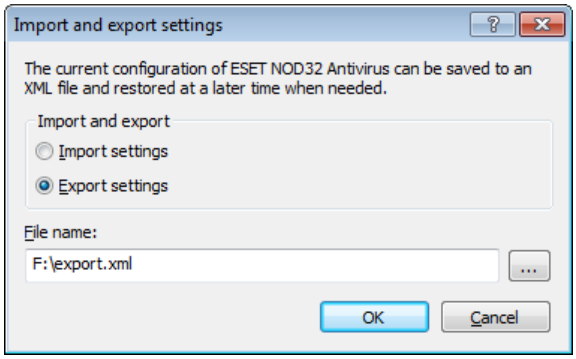
5.2 Import and export settings

Importing and exporting configurations of ESET NOD32 Antivirus is available under **Setup**.

Both import and export use the *.xml* file type. Import and export are useful if you need to backup the current configuration of ESET NOD32 Antivirus to be able to use it later. The export settings option is also convenient for users who wish to use their preferred configuration of ESET NOD32 Antivirus on multiple systems – they can easily import an .xml file to transfer the desired settings.

Importing a configuration is very easy. From the main menu, click **Setup** > **Import and export settings...**, and then select the **Import settings** option. Enter the path of the configuration file or click the **...** button to browse for the configuration file you wish to import.

The steps to export a configuration are very similar. From the main menu, click **Setup** > **Import and export settings...**. Select the **Export settings** option and enter the **File name** of the configuration file (i.e. *export.xml*). Use the browser to select a location on your computer to save the configuration file.



5.3 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET NOD32 Antivirus include:

Ctrl+G	disables GUI in the product
Ctrl+I	opens the ESET SysInspector page
Ctrl+L	opens the Log files page
Ctrl+S	opens the Scheduler page
Ctrl+Q	opens the Quarantine page
Ctrl+U	opens a dialog window where Username and Password can be set

For better navigation in the ESET security product, the following keyboard shortcuts can be used:

F1	opens help pages
F5	opens the Advanced setup
Up/Down	navigation in product though items
*	expands the Advanced setup tree node
-	collapses the Advanced setup tree node
TAB	moves the cursor in a window
Esc	closes the active dialog window

5.4 Command Line

ESET NOD32 Antivirus's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file. ESET Command-line scanner usage:

```
ecls [OPTIONS..] FILES..
```

The following parameters and switches can be used while running the on-demand scanner from the command line:

Options

/base-dir=FOLDER	load modules from FOLDER
/quar-dir=FOLDER	quarantine FOLDER
/exclude=MASK	exclude files matching MASK from scanning
/subdir	scan subfolders (default)
/no-subdir	do not scan subfolders
/max-subdir-level=LEVEL	maximum sub-level of folders within folders to scan
/symlink	follow symbolic links (default)
/no-symlink	skip symbolic links
/ads	scan ADS (default)
/no-ads	do not scan ADS
/log-file=FILE	log output to FILE
/log-rewrite	overwrite output file (default – append)
/log-console	log output to console (default)
/no-log-console	do not log output to console
/log-all	also log clean files
/no-log-all	do not log clean files (default)
/aind	show activity indicator
/auto	scan and automatically clean all local disks

Scanner options

/files	scan files (default)
/no-files	do not scan files
/memory	scan memory
/boots	scan boot sectors
/no-boots	do not scan boot sectors (default)
/arch	scan archives (default)
/no-arch	do not scan archives
/max-obj-size=SIZE	only scan files smaller than SIZE megabytes (default 0 = unlimited)
/max-arch-level=LEVEL	maximum sub-level of archives within archives (nested archives) to scan
/scan-timeout=LIMIT	scan archives for LIMIT seconds at maximum
/max-arch-size=SIZE	only scan the files in an archive if they are smaller than SIZE (default 0 = unlimited)

/max-sfx-size=SIZE	only scan the files in a self-extracting archive if they are smaller than SIZE megabytes (default 0 = unlimited)
/mail	scan email files (default)
/no-mail	do not scan email files
/mailbox	scan mailboxes (default)
/no-mailbox	do not scan mailboxes
/sfx	scan self-extracting archives (default)
/no-sfx	do not scan self-extracting archives
/rtp	scan runtime packers (default)
/no-rtp	do not scan runtime packers
/adware	scan for Adware/Spyware/Riskware (default)
/no-adware	do not scan for Adware/Spyware/Riskware
/unsafe	scan for potentially unsafe applications
/no-unsafe	do not scan for potentially unsafe applications (default)
/unwanted	scan for potentially unwanted applications
/no-unwanted	do not scan for potentially unwanted applications (default)
/pattern	use signatures (default)
/no-pattern	do not use signatures
/heur	enable heuristics (default)
/no-heur	disable heuristics
/adv-heur	enable Advanced heuristics (default)
/no-adv-heur	disable Advanced heuristics
/ext=EXTENSIONS	scan only EXTENSIONS delimited by colon
/ext-exclude=EXTENSIONS	exclude EXTENSIONS delimited by colon from scanning
/clean-mode=MODE	use cleaning MODE for infected objects. Available options: none, standard (default), strict, rigorous, delete
/quarantine	copy infected files (if cleaned) to Quarantine (supplements ACTION)
/no-quarantine	do not copy infected files to Quarantine

General options

/help	show help and quit
/version	show version information and quit
/preserve-time	preserve last access timestamp

Exit codes

0	no threat found
1	threat found and cleaned
10	some files could not be scanned (may be threats)
50	threat found
100	error

NOTE: Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

5.5 ESET SysInspector

5.5.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET NOD32 Antivirus or by downloading the standalone version (SysInspector.exe) for free from ESET's website. To open ESET SysInspector, click **Tools** > **ESET SysInspector**. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The downloaded and integrated versions each allow you to export system snapshots to an .xml file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (for more information see section ESET SysInspector as part of ESET NOD32 Antivirus).

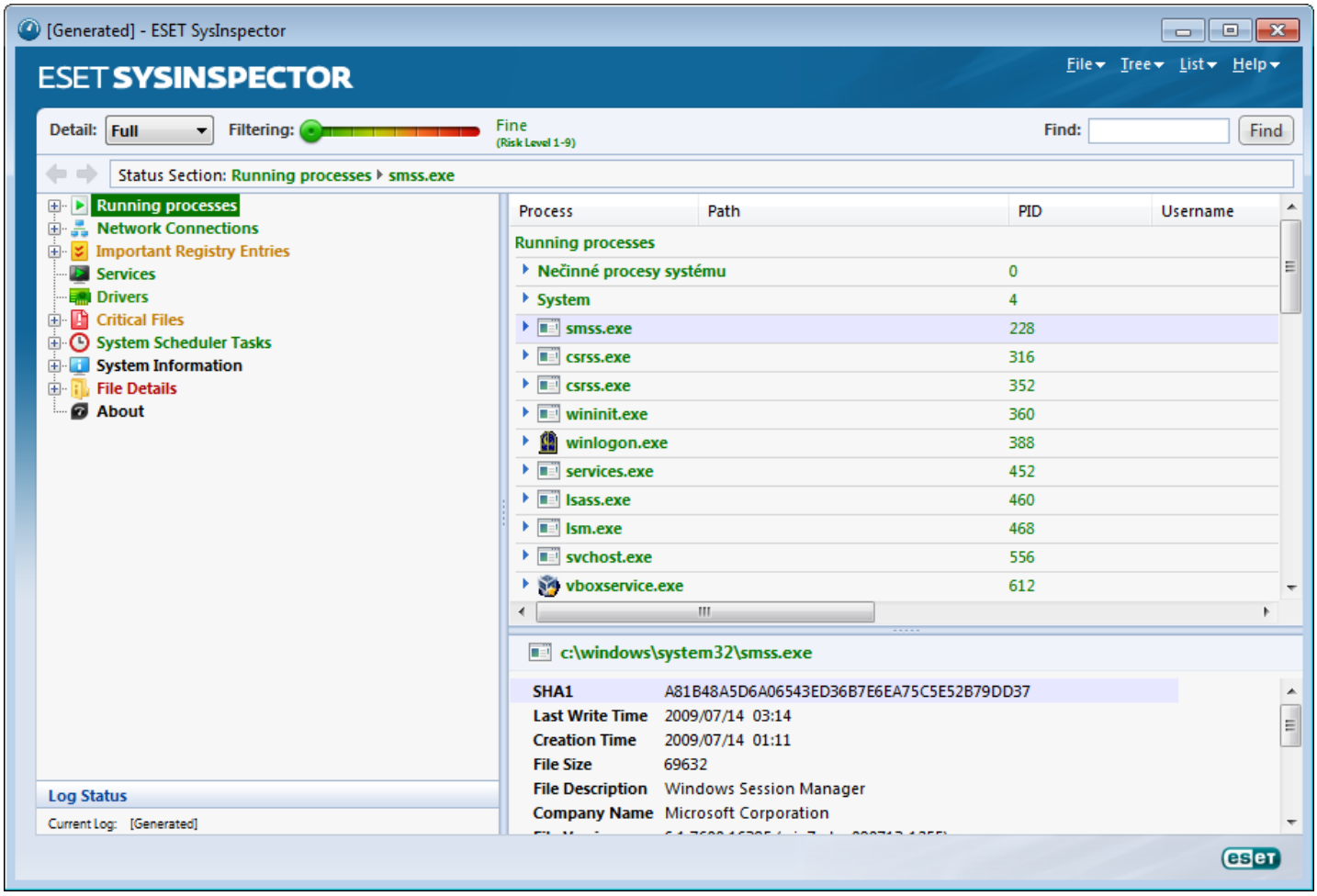
Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

5.5.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website. If you already have one of the ESET security products installed, you can run ESET SysInspector directly from the Start Menu (**Programs** > **ESET** > **ESET NOD32 Antivirus**). Please wait while the application inspects your system, which could take up to several minutes depending on your hardware and data to be gathered.

5.5.2 User Interface and application usage

For clarity the Main window is divided into four major sections – Program Controls located on the top of the Main window, the Navigation window on the left, the Description window on the right in the middle and the Details window on the right at the bottom of the Main window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



5.5.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by simply dragging and dropping them into the Main window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the Main window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Item filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current Risk Level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the Risk Level slider.

Search

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return

By clicking the back or forward arrow, you may return to previously displayed information in the Description window. You may use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

5.5.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or alternatively click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system comprises of several important kernel components running 24/7 that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical files

The Description window displays content of critical files related to the Microsoft windows operating system.

System information

Contains detailed information about hardware and software along with information about set environmental variables and user rights.

File details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about ESET SysInspector.

5.5.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting activity of malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Navigate to **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, use **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, use the option **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

NOTE: If you compare two log files, select **File** > **Save log** to save it as a ZIP file; both files are saved. If you open this file later, the contained logs are automatically compared.

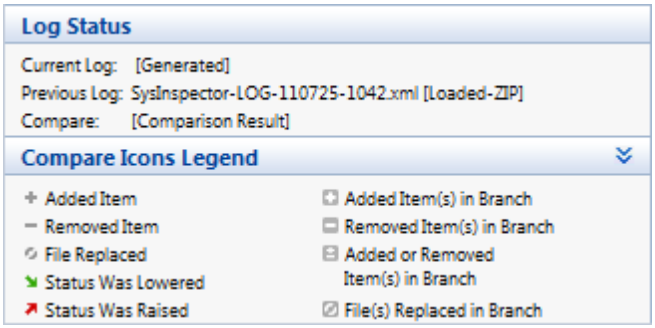
Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Items marked by a – can only be found in the active log and were not present in the opened comparative log. Items marked by a + were present only in the opened log and are missing in the active one.

Description of all symbols that can be displayed next to items:

- new value, not present in the previous log
- tree structure section contains new values
- removed value, present in the previous log only
- tree structure section contains removed values
- value / file has been changed
- tree structure section contains modified values / files
- the risk level has decreased / it was higher in the previous log
- the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, navigate to **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

SysIsnpector.exe current.xml previous.xml

5.5.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen	generate a log directly from the command line without running the GUI
/privacy	generate a log excluding sensitive information
/zip	store the resulting log directly on the disk in a compressed file
/silent	suppress the display of the log generation progress bar
/help, /?	display information about the command line parameters

Examples

To load a specific log directly in the browser, use: *SysInspector.exe "c:\clientlog.xml"*
To generate a log to a current location, use: *SysInspector.exe /gen*
To generate a log to a specific folder, use: *SysInspector.exe /gen="c:\folder\"*
To generate a log to a specific file/location, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
To generate a log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
To compare two logs, use: *SysInspector.exe "current.xml" "original.xml"*

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

5.5.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspectorby easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you have a suspicion that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

- Run ESET SysInspector to generate a new system snapshot.
- Select the first item in the section on the left (in the tree structure), press Ctrl and select the last item to mark all items.
- Right click the selected objects and select the **Export Selected Sections To Service Script** context menu option.
- The selected objects will be exported to a new log.
- This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
- Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
- Click **OK** to run the script.

5.5.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either the **Export All Sections To Service Script** option or the **Export Selected Sections To Service Script** option.

NOTE: It is not possible to export the service script when two logs are being compared.

5.5.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

The services marked and their dependant services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be unregistered from the system and removed.

09) Critical files

This section contains information about files that are critical to the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

5.5.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

5.5.5 Shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O	opens existing log
Ctrl+S	saves created logs

Generate

Ctrl+G	standard system status check
Ctrl+H	performs a system check that may also log sensitive information

Item Filtering

1, O	fine, risk level 1-9 items are displayed
2	fine, risk level 2-9 items are displayed
3	fine, risk level 3-9 items are displayed
4, U	unknown, risk level 4-9 items are displayed
5	unknown, risk level 5-9 items are displayed
6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+O	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item

Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor
Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field
Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help
Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

5.5.6 System requirements

For seamless operation of ESET SysInspector, the system should meet the following hardware and software requirements:

Windows 2000, XP, 2003

400 MHz 32-bit (x86) / 64-bit (x64)
128MB RAM of system memory
10MB available space
Super VGA (800 x 600)

Windows 7, Vista, 2008

1 GHz 32-bit (x86) / 64-bit (x64)
512MB RAM of system memory
10MB available space
Super VGA (800 x 600)

5.5.7 FAQ

Does ESET SysInspector require Administrator privileges to run ?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file ?

ESET SysInspector can create a log file of your computer's configuration. To save one, select **File** > **Save Log** from the main menu. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file ?

To view a log file created by ESET SysInspector, run the program and select **File** > **Open Log** from the main menu. You

can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK ?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object ?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous ?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run ?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology ?

Anti-Stealth technology provides effective rootkits detection.

If the system is attacked by malicious code that behaves as a rootkit, the user is exposed to the risk of damage or theft of data. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time ?

When trying to identify the digital signature of an executable file, ESET SysInspector first seeks whether there is a digital signature embedded in the file. In this the, case the identification within the file will be used when validating. Should the file not contain a digital signature, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%\system32\catroot*) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in *C:\Program Files\Windows NT*. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* pointing to *C:\Program Files\Windows NT\hypertrm.exe* (the main executable of the HyperTerminal application) and *sp4.cat* is digitally signed by Microsoft.

5.5.8 ESET SysInspector as part of ESET NOD32 Antivirus

To open the ESET SysInspector section in ESET NOD32 Antivirus, click **Tools** > **ESET SysInspector**. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To **Compare**, **Create...**, or **Delete** snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, use the **View** context menu option. To export the selected snapshot to a file, right-click it and select **Export...**
.

Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.
- **Add** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.
- **Remove** – Removes entries from the list.
- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

5.6 ESET SysRescue

ESET SysRescue is a utility which enables you to create a bootable disk containing ESET NOD32 Antivirus. The main advantage of ESET SysRescue is the fact that ESET NOD32 Antivirus runs independent of the host operating system, while it has a direct access to the disk and the entire file system. This makes it possible to remove infiltrations which normally could not be deleted, e.g., when the operating system is running, etc.

5.6.1 Minimun requirements

ESET SysRescue works in the Microsoft Windows Preinstallation Environment (Windows PE) version 2.x, which is based on Windows Vista. Windows PE is a part of the free package Windows Automated Installation Kit (Windows AIK), and therefore Windows AIK must be installed before creating ESET SysRescue (http://go.eset.eu/AIK). Due to the support of the 32-bit version of Windows PE, it is necessary to use a 32-bit ESET NOD32 Antivirus installation package when creating ESET SysRescue on 64-bit systems. ESET SysRescue supports Windows AIK 1.1 and higher. ESET SysRescue is available in ESET NOD32 Antivirus 4.0 and higher.

Supported operating systems

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 with KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 with KB926044
- Windows XP Service Pack 3

5.6.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start** > **Programs** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

First, the wizard checks for the presence of Windows AIK and a suitable device for the boot media creation. If *Windows AIK* is not installed on the computer (or it is either corrupt or installed incorrectly), the wizard will offer you the option to install it, or to enter the path to your Windows AIK folder (http://go.eset.eu/AIK).

In the next step, select the target media where ESET SysRescue will be located.

5.6.3 Target selection

In addition to CD/DVD/USB, you can choose to save ESET SysRescue in an ISO file. Later on, you can burn the ISO image on CD/DVD, or use it some other way (e.g. in the virtual environment such as VMware or VirtualBox).

If you select USB as the target medium, booting may not work on certain computers. Some BIOS versions may report problems with the BIOS - boot manager communication (e.g. on Windows Vista) and booting exits with the following error message:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data
```

If you encounter this message, we recommend selecting CD instead of USB medium.

5.6.4 Settings

Before initiating ESET SysRescue creation, the install wizard displays compilation parameters in the last step of the ESET SysRescue wizard. These can be modified by clicking the **Change...** button. The available options include:

- Folders
- ESET Antivirus
- Advanced
- Internet protocol
- Bootable USB device (when the target USB device is selected)
- Burning (when the target CD/DVD drive is selected)

The **Create** button is inactive if no MSI installation package is specified, or if no ESET security solution is installed on the computer. To select an installation package, click the **Change** button and go to the **ESET Antivirus** tab. Also, if you do not fill in username and password (**Change** > **ESET Antivirus**), the **Create** button is greyed out.

5.6.4.1 Folders

Temporary folder is a working directory for files required during ESET SysRescue compilation.

ISO folder is a folder, where the resulting ISO file is saved after the compilation is completed.

The list on this tab shows all local and mapped network drives together with the available free space. If some of the folders here are located on a drive with insufficient free space, we recommend that you select another drive with more free space available. Otherwise compilation may end prematurely due to insufficient free disk space.

External applications – Allows you to specify additional programs that will be run or installed after booting from a ESET SysRescue medium.

Include external applications – Allows you to add external programs to the ESET SysRescue compilation.

Selected folder – Folder in which programs to be added to the ESET SysRescue disk are located.

5.6.4.2 ESET Antivirus

For creating the ESET SysRescue CD, you can select two sources of ESET files to be used by the compiler.

ESS/EAV folder – Files already contained in the folder to which the ESET product is installed on the computer.

MSI file – Files contained in the MSI installer are used.

Next, you can choose to update the location of (.nup) files. Normally, the default option **ESS/EAV folder/MSI file** should be set. In some cases, a custom **Update folder** can be chosen, e.g., to use an older or newer virus signature database version.

You can use one of the following two sources of username and password:

Installed ESS/EAV – Username and password will be copied from the currently installed ESET NOD32 Antivirus.

From user – User name and password entered in the corresponding text boxes will be used.

NOTE: ESET NOD32 Antivirus on the ESET SysRescue CD is updated either from the Internet or from the ESET Security solution installed on the computer on which the ESET SysRescue CD is run.

5.6.4.3 Advanced settings

The **Advanced** tab lets you optimize the ESET SysRescue CD according to the amount of memory on your computer. Select **576 MB and more** to write the content of the CD to the operating memory (RAM). If you select **less than 576 MB** , the recovery CD will be permanently accessed when WinPE will be running.

In the **External drivers** section, you can insert drivers for your specific hardware (usually network adapter). Although WinPE is based on Windows Vista SP1, which supports a large range of hardware, occasionally hardware is not recognized. This will required that you add a driver manually. There are two ways of introducing a driver into an ESET SysRescue compilation - manually (the **Add** button) and automatically (the **Aut. Search** button). In the case of manual inclusion, you need to select the path to the corresponding .inf file (applicable *.sys file must also be present in this folder). In the case of automatic introduction, the driver is found automatically in the operating system of the given computer. We recommend using automatic inclusion only if ESET SysRescue is used on a computer that has the same network adapter as the computer on which the ESET SysRescue CD was created. During creation, the ESET SysRescue

driver is introduced into the compilation so you do not need to look for it later.

5.6.4.4 Internet protocol

This section allows you to configure basic network information and set up predefined connections after ESET SysRescue.

Select **Automatic private IP address** to obtain the IP address automatically from DHCP (Dynamic Host Configuration Protocol) server.

Alternatively, this network connection can use a manually specified IP address (also known as a static IP address). Select **Custom** to configure the appropriate IP settings. If you select this option, you must specify an **IP address** and, for LAN and high-speed Internet connections, a **Subnet mask**. In **Preferred DNS server** and **Alternate DNS server**, type the primary and secondary DNS server addresses.

5.6.4.5 Bootable USB device

If you have selected a USB device as your target medium, you can select one of the available USB devices on the **Bootable USB device** tab (in case there are more USB devices).

Select the appropriate target **Device** where ESET SysRescue will be installed.

Warning: The selected USB device will be formatted during the creation of ESET SysRescue. All data on the device will be deleted.

If you choose the **Quick format** option, formatting removes all the files from the partition, but does not scan the disk for bad sectors. Use this option if your USB device has been formatted previously and you are sure that it is not damaged.

5.6.4.6 Burn

If you have selected CD/DVD as your target medium, you can specify additional burning parameters on the **Burn** tab.

Delete ISO file – Check this option to delete the temporary ISO file after the ESET SysRescue CD is created.

Deletion enabled – Enables you to select fast erasing and complete erasing.

Burning device – Select the drive to be used for burning.

Warning: This is the default option. If a rewritable CD/DVD is used, all the data on the CD/DVD will be erased.

The Medium section contains information about the medium in your CD/DVD device.

Burning speed – Select the desired speed from the drop-down menu. The capabilities of your burning device and the type of CD/DVD used should be considered when selecting the burning speed.

5.6.5 Working with ESET SysRescue

For the rescue CD/DVD/USB to work effectively, you must start your computer from the ESET SysRescue boot media. Boot priority can be modified in the BIOS. Alternatively, you can use the boot menu during computer startup – usually using one of the F9 - F12 keys depending on the version of your motherboard/BIOS.

After booting up from the boot media, ESET NOD32 Antivirus will start. Since ESET SysRescue is used only in specific situations, some protection modules and program features present in the standard version of ESET NOD32 Antivirus are not needed; their list is narrowed down to **Computer scan**, **Update**, and some sections in **Setup**. The ability to update the virus signature database is the most important feature of ESET SysRescue, we recommend that you update the program prior starting a Computer scan.

5.6.5.1 Using ESET SysRescue

Suppose that computers in the network have been infected by a virus which modifies executable (.exe) files. ESET NOD32 Antivirus is capable of cleaning all infected files except for *explorer.exe*, which cannot be cleaned, even in Safe mode.

This is because *explorer.exe*, as one of the essential Windows processes, is launched in Safe mode as well. ESET NOD32 Antivirus would not be able to perform any action with the file and it would remain infected.

In this type of scenario, you could use ESET SysRescue to solve the problem. ESET SysRescue does not require any component of the host operating system, and is therefore capable of processing (cleaning, deleting) any file on the disk.

6. Glossary

6.1 Types of infiltration

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

6.1.1 Viruses

A computer virus is a piece of malicious code that is pre-pended or appended to existing files on your computer. Viruses are named after biological viruses because they use similar techniques to spread from one computer to another. As for the term "virus", it is often used incorrectly to mean any type of a threat. This usage is gradually being overcome and replaced with a more accurate term "malware" (malicious software).

Computer viruses mainly attack executable files and documents. In short, this is how a computer virus works: after execution of an infected file, the malicious code is called and executed prior to the execution of the original application. A virus can infect any files that the current user has write permissions for.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

If your computer is infected with a virus and cleaning is not possible, submit it to the ESET lab for perusal. In certain cases infected files can be modified to such an extent that cleaning is not possible and the files must be replaced with a clean copy.

6.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via network. The basic difference between a virus and a worm is that worms have the ability to propagate by themselves; they are not dependant on host files (or boot sectors). Worms spread to email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes after their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

6.1.3 Trojan horses

Historically, computer Trojans (Trojan horses) have been defined as a class of threats which attempt to present themselves as useful programs and thus trick users into running them.

Since Trojans are a very broad category, it is often divided into several subcategories:

- **Downloader** – Malicious programs with the ability to download other threats from the Internet.
- **Dropper** – Malicious programs with the ability to drop other types of malware onto compromised computers.
- **Backdoor** – Malicious programs which communicate with remote attackers, allowing them to gain access to the computer and take control over it.
- **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers.
- **Dialer** – Malicious programs designed to connect via premium-rate numbers instead of the user's Internet service provider. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

If a file on your computer is detected as a Trojan, it is advisable to delete it, since it most likely contains nothing but malicious code.

6.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1. When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2. When they are hidden from the usual testing. ESET NOD32 Antivirus users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

6.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

6.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET NOD32 Antivirus provides the option to detect such threats.

"Potentially unsafe applications" is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

6.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously (pop-ups, ads),
- Activating and running of hidden processes,
- Increased usage of system resources,
- Changes in search results,
- Application communicates with remote servers.

6.2 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms – be especially cautious of options such as "Yes, I want to receive information".
- Use "specialized" email addresses – e.g., one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

6.2.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

6.2.2 Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

6.2.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

6.2.4 Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message.

- Sender address does not belong to someone on your contact list.
- You are offered a large sum of money, but you have to provide a small sum first.
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- It is written in a foreign language.
- You are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer).
- Some of the words are misspelled in an attempt to trick your spam filter. For example “vaigra” instead of “viagra”, etc.